



---

# JunosE™ Software for E Series™ Broadband Services Routers

## System Event Logging Reference Guide

Release

13.3.x



---

Published: 2012-09-12

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*JunosE™ Software for E Series™ Broadband Services Routers System Event Logging Reference Guide*  
Release 13.3.x  
Copyright © 2012, Juniper Networks, Inc.  
All rights reserved.

Revision History  
October 2012—FRS JunosE 13.3.x

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Abbreviated Table of Contents

	About the Documentation .....	xvii
Part 1	Chapters	
Chapter 1	System Logging Overview .....	3
Chapter 2	Event Categories .....	21
Part 2	Event Categories	
Chapter 3	A Commands .....	25
Chapter 4	B Commands .....	35
Chapter 5	C Commands .....	51
Chapter 6	D Commands .....	57
Chapter 7	E Commands .....	79
Chapter 8	F Commands .....	81
Chapter 9	G and H Commands .....	87
Chapter 10	I Commands .....	91
Chapter 11	L Commands .....	129
Chapter 12	M Commands .....	145
Chapter 13	N Commands .....	165
Chapter 14	O Commands .....	169
Chapter 15	P Commands .....	193
Chapter 16	Q Commands .....	213
Chapter 17	R Commands .....	215
Chapter 18	S Commands .....	229
Chapter 19	T Commands .....	247
Chapter 20	U Commands .....	255
Chapter 21	V Commands .....	257
Part 3	Index	
	Index .....	263



# Table of Contents

	<b>About the Documentation</b> . . . . .	<b>xvii</b>
	E Series and JunosE Documentation and Release Notes . . . . .	xvii
	Audience . . . . .	xvii
	E Series and JunosE Text and Syntax Conventions . . . . .	xvii
	Obtaining Documentation . . . . .	xix
	Documentation Feedback . . . . .	xix
	Requesting Technical Support . . . . .	xix
	Self-Help Online Tools and Resources . . . . .	xx
	Opening a Case with JTAC . . . . .	xx
<b>Part 1</b>	<b>Chapters</b>	
<b>Chapter 1</b>	<b>System Logging Overview</b> . . . . .	<b>3</b>
	Overview of System Logging . . . . .	3
	Log Severity . . . . .	3
	Log Verbosity . . . . .	4
	Persistent Logs . . . . .	4
	Logging Platform Considerations . . . . .	5
	Configuring Event Logging . . . . .	5
	Configuring Log Severity for Individual and Systemwide Logs . . . . .	10
	Configuring Log Verbosity for Individual Logs or All Logs . . . . .	13
	Setting the Timestamp for Log Messages . . . . .	14
	Configuring Log Filters . . . . .	15
	Turning Off Log Filters . . . . .	16
	Monitoring Logging System Events . . . . .	16
<b>Chapter 2</b>	<b>Event Categories</b> . . . . .	<b>21</b>
<b>Part 2</b>	<b>Event Categories</b>	
<b>Chapter 3</b>	<b>A Commands</b> . . . . .	<b>25</b>
	aaaAtm1483Cfg . . . . .	25
	aaaEngineGeneral . . . . .	26
	aaaQosCfg . . . . .	26
	aaaServerGeneral . . . . .	27
	aaaUserAccess . . . . .	28
	addressServerGeneral . . . . .	28
	ar1AaaServerGeneral . . . . .	29
	atm . . . . .	29
	atm1483 . . . . .	30
	atm1483VcClass . . . . .	31
	atmAal5 . . . . .	31





igmpGeneral	95
igmpGracefulRestart	96
igmpGroupState	97
ikeCertificateMgr	97
ikeEnrollment	98
ikepi	98
interModuleCommunication	99
ipAccessList	100
ipEngine	100
ipEngineering	101
ipflowstats	101
ipflowstatsEngine	102
ipGeneral	102
ipIfCreator	104
ipInterface	104
ipNhopTrackerGeneral	105
ipProfileMgr	105
ipRoutePolicy	106
ipRouteTable	106
ipseclDb	107
ipsecPIThrottler	107
ipsecXcfgSM	108
ipSubscriberMgr	108
ipTraffic	109
ipTunnel	109
ipv6AccessList	110
ipv6Engineering	111
ipv6General	111
ipv6Interface	112
ipv6ProfileMgr	113
ipv6RouteTable	113
ipv6Traffic	114
ipv6Types	115
isisAdjChange	115
isisAdjPackets	116
isisBfdEvents	117
isisChecksumErr	117
isisGeneral	118
isisHelloGeneral	118
isisHelloPackets	119
isisIpv6Log	119
isisLdpEvents	120
isisLocalUpdate	120
isisMplsTeAdvertisements	121
isisMplsTeEvents	122
isisNsfEvents	122
isisProtocolErr	123
isisSnppackets	123
isisSpfEvents	124









	tcpTraffic .....	248
	tcpv6Traffic .....	249
	telnet .....	250
	telnetClient .....	250
	tftpClient .....	251
	trackerEvents .....	251
	trackerGeneral .....	252
	tsm .....	252
<b>Chapter 20</b>	<b>U Commands .....</b>	<b>255</b>
	udpTraffic .....	255
	udpv6Traffic .....	256
<b>Chapter 21</b>	<b>V Commands .....</b>	<b>257</b>
	vrrp .....	257
	vrrpTracking .....	258
	vsm .....	258
	vsmEngine .....	259
<b>Part 3</b>	<b>Index</b>	
	Index .....	263



# List of Tables

	<b>About the Documentation . . . . .</b>	<b>xvii</b>
	Table 1: Notice Icons . . . . .	xviii
	Table 2: Text and Syntax Conventions . . . . .	xviii
<b>Part 1</b>	<b>Chapters</b>	
<b>Chapter 1</b>	<b>System Logging Overview . . . . .</b>	<b>3</b>
	Table 3: Log Severity Descriptions . . . . .	4



# About the Documentation

- E Series and JunosE Documentation and Release Notes on page xvii
- Audience on page xvii
- E Series and JunosE Text and Syntax Conventions on page xvii
- Obtaining Documentation on page xix
- Documentation Feedback on page xix
- Requesting Technical Support on page xix

## E Series and JunosE Documentation and Release Notes

---

For a list of related JunosE documentation, see  
<http://www.juniper.net/techpubs/software/index.html>.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE Release Notes*.

To obtain the most current version of all Juniper Networks<sup>®</sup> technical documentation, see the product documentation page on the Juniper Networks website at  
<http://www.juniper.net/techpubs/>.

## Audience

---

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

## E Series and JunosE Text and Syntax Conventions

---

Table 1 on page xviii defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xviii defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents commands and keywords in text.	<ul style="list-style-type: none"> <li>Issue the <b>clock source</b> command.</li> <li>Specify the keyword <b>exp-msg</b>.</li> </ul>
<b>Bold text like this</b>	Represents text that the user must type.	<b>host1(config)#traffic class low-loss1</b>
Fixed-width text like this	Represents information as displayed on your terminal's screen.	<b>host1#show ip ospf 2</b>  Routing Process OSPF 2 with Router ID 5.5.0.250  Router is an Area Border Router (ABR)
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Emphasizes words.</li> <li>Identifies variables.</li> <li>Identifies chapter, appendix, and book names.</li> </ul>	<ul style="list-style-type: none"> <li>There are two levels of access: <i>user</i> and <i>privileged</i>.</li> <li><i>clusterId</i>, <i>ipAddress</i>.</li> <li><i>Appendix A, System Specifications</i></li> </ul>
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<b>Syntax Conventions in the Command Reference Guide</b>		
Plain text like this	Represents keywords.	terminal length
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic   line
[ ] (brackets)	Represent optional keywords or variables.	[ internal   external ]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[ level1   level2   l1 ]*
{ } (braces)	Represent required keywords or variables.	{ permit   deny } { in   out }  { clusterId   ipAddress }

## Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at <http://www.juniper.net/>.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

<http://www.juniper.net/techpubs/resources/index.html>

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site at <http://www.juniper.net/>.

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,



## PART 1

# Chapters

- [System Logging Overview on page 3](#)
- [Event Categories on page 21](#)



## CHAPTER 1

# System Logging Overview

E Series Broadband Services Routers enable you to log system events to discover and isolate problems with your system. This chapter explains how to use the command-line interface (CLI) to monitor your system's log configuration and stay informed about all system events that you want to track.

This chapter contains the following sections:

- [Overview of System Logging on page 3](#)
- [Logging Platform Considerations on page 5](#)
- [Configuring Event Logging on page 5](#)
- [Configuring Log Severity for Individual and Systemwide Logs on page 10](#)
- [Configuring Log Verbosity for Individual Logs or All Logs on page 13](#)
- [Setting the Timestamp for Log Messages on page 14](#)
- [Configuring Log Filters on page 15](#)
- [Turning Off Log Filters on page 16](#)
- [Monitoring Logging System Events on page 16](#)

## Overview of System Logging

---

System events are classified into event categories. Using the CLI, you can determine which event categories to log. To fully utilize the logging facility, you need to understand *log severity* and *log verbosity*.

### Log Severity

Log severity is a level that is assigned to an event or log message. Log severity levels apply to event categories, such as `bulkStats`, `bgpRoutes`, or `atm1483`.

The minimum severity of a log message for an individual category is described either by a severity number in the range 0–7 or a descriptive priority term, such as *emergency* or *debug*. The lower the severity number is, the higher the priority. See [Table 3 on page 4](#).



**NOTE:** Not every event category supports every severity level. For a list of event categories and the severity levels that each category supports, see [“Event Categories” on page 21](#).

**Table 3: Log Severity Descriptions**

Severity Number	Severity Name	System Response
0	Emergency	System unusable; shelf reset
1	Alert	Immediate action needed; card reset
2	Critical	Critical conditions exist; interface is down
3	Error	Error conditions; nonrecoverable software error
4	Warning	Warning conditions; recoverable software error
5	Notice	Normal but significant conditions; nonerror, low-verbosity information
6	Info	Informational messages; nonerror, medium-verbosity information
7	Debug	Debug messages; nonerror, high-verbosity information

## Log Verbosity

The verbosity level determines the amount of information that appears in each message. You can assign the verbosity level for the log category. Verbosity levels can be any of the following:

- Low—Terse
- Medium—Moderate
- High—Verbose



**NOTE:** Many event categories provide only low-verbosity detail regardless of the verbosity setting.

## Persistent Logs

Log messages can survive a system reboot. After a reboot, the system rebuilds the list of log messages. However, if the system detects any problems or has gone through a power cycle, the buffer is reset, and the log messages from the previous session are lost.



*Hour:Minute[:Second]*—Current time in 24-hour format. Seconds are optional.

- **utc**—Enter this keyword to indicate that the time entered is in universal coordinated time (UTC), rather than local time.
- To set a specific date, use the following syntax:

*Month Day Year*—You must spell out the name of the month.

- **last-reset**—Causes the system to display log messages generated since the last time the system was reset
- Examples

```
host1#baseline log 11:12:55 April 30 2002
host1#baseline log last-reset
```

- There is no **no** version.
- See baseline log.

- log destination**
- Use to log messages to the specified destination, including system log, console, and nv-file (nonvolatile storage).



**NOTE:** You can display traffic logs—such as ipTraffic, icmpTraffic, tcpTraffic, and udpTraffic—only through the **show log data** command or from the SRP module console. You cannot redirect traffic logs elsewhere, such as to a system log or nonvolatile storage file, or to a Telnet session.

- Use the **severity** keyword to limit the messages logged based on priority level.
- The following information applies to logging messages to system log servers.
  - You can have multiple system log servers, but must configure logging to each one separately.
  - A particular message within a specified event category is logged to a particular system log server only if the priority of the message is greater than or equal to both the priority of the event category and the priority of that system log server.
  - If you log messages to a system log server, you can also specify:
    - **facility**—Specifies a facility ID on the system log destination host. The range is 0–7, representing the logging facilities local0–local7.
    - **include**—Logs only the listed categories to system log; no other categories are logged unless specifically included by issuing this command again.
    - **exclude**—Logs all categories to system log except the listed categories; all other categories are logged unless specifically excluded by issuing this command again.
  - Issuing an **include** command after an **exclude** command (or vice versa) overrides the earlier command. Therefore, you cannot enter a command including certain categories and then follow it with a command excluding others. Similarly, you cannot



- log destination syslog source**
- Use to specify a source interface type and location for events logged to system log at the specified IP address.
  - Overrides the actual source interface type and location. The IP address associated with the specified source interface is used as the source address for subsequent system log messages.
  - Example  
`host1(config)#log destination syslog 10.1.2.3 source atm 0/1`
  - Use the **no** version to restore the actual source interface type and location.
  - See log destination syslog source.
- log engineering**
- Use to enable engineering logs.
  - Provides troubleshooting information to assist you when contacting Juniper Networks Technical Assistance Center (JTAC).
  - Example  
`host1(config)#log engineering`
  - Use the **no** form of this command to disable engineering logs.
  - See log engineering.
- log fields**
- Use to select fields to be added to all logs. These fields include a timestamp for the message, an instance identifier, and the name of the internal software application that created the message.
  - Example  
`host1(config)#log fields timestamp instance no-calling-task`
  - Use the **no** version to restore the default log field settings.
  - See log fields.
- log here**
- Use to enable logs destined for a console to be displayed at the current console.
  - By default, the local console automatically receives all log messages if console is a destination. The exception is the cliCommand log, whose log events do not appear on the console.
  - By default, Telnet consoles do not receive log messages.
  - Example  
`host1#log here`
  - Use the **no** version to disable logs destined for a console from being displayed on this console.
  - See log here.

- log severity**
- Use to set the severity level for systemwide logs (that is, when you do not specify an individual event category) or for a specific event category. For a list of severity values, see [Table 3 on page 4](#).



**NOTE:** Assigning a log severity to an individual event category changes its state to Assigned. You cannot change the severity of that event category using systemwide level commands until you return the event category to its default, unassigned state with the **no log severity** command.

- If you do not specify a category, the severity value changes for all categories except individual categories for which you previously set a specific severity level. See [“Configuring Log Severity for Individual and Systemwide Logs” on page 10](#) for details.
- Each event category has its own default severity value. For most categories, the default is Error.
- To disable all *default* level log messages, use the **off** keyword without specifying an event category.
- To disable individual level log messages, use the **off** keyword and specify the event category that you want to disable.
- Example
 

```
host1(config)#log severity warning
```
- Use the **no** version to return the systemwide (when assigned) or default severity values to event categories.
- Use the **no** version with an\* (asterisk) to return all event categories (modified either systemwide or individually) to their default severity setting. For example:
 

```
host1(config)#no log severity *
```
- See log severity.

- log unlimited**
- Use to remove the limit on the number of outstanding buffers for an event category, such as when the system is dropping logs of a particular category.
  - Example
 

```
host1(config)#log unlimited qos
```
  - Use the **no** version to return to the default value.
  - See log unlimited.

- log verbosity**
- Use to set the verbosity level for a selected category or for all categories.
  - If you do not specify a category, then the verbosity level is set for all categories.
  - The default verbosity setting for all logs is low.
  - Example
 

```
host1(config)#log verbosity low
```

- Use the **no** version to return to the default verbosity (low) for the selected category.
- See log verbosity.

## Configuring Log Severity for Individual and Systemwide Logs

---

You can change the severity setting for *individual* logs and the *systemwide* value.

When working with log severities, keep the following in mind:

- All log event categories have a default. However, the default values can vary for each category. For example, most event categories have a default severity of Error. However, some event categories may have a default severity of Notice, Warning, Info, and so on.
- Log event categories have two states—unassigned (default) and assigned. How a log event category reacts to the **log severity** command depends on its current state.
- You can change log severities for event categories at a systemwide level or an individual level. Systemwide changes are those that modify a large number of unassigned event categories at one time; for example, the command **log severity debug off**. Individual changes are those that indicate an explicit event category that you want to change; for example, the command **log severity notice clicommand**.
- Changes to log event categories at an individual level take precedence over those made at the systemwide level.
- Changes to log event categories at the systemwide level take precedence over the default.
- Assigning a log severity to an individual event category changes its state to Assigned. This means that you cannot change the severity of that event category using systemwide level commands until you return the event category to its default, unassigned state by using the **no log severity eventCategory** command.
- To return all logs, systemwide and individual, to their default, unassigned severity level, use the **no log severity \*** command.
- To see whether individual or systemwide severity and verbosity settings are in effect, use the **show log configuration** command.

**Example** The following example demonstrates the effects of event category state in regard to using systemwide commands:

1. In Configuration mode and having made no changes to the severity settings of any event categories, view the log configuration:

```
host1(config)#run show log config
log destination console severity WARNING
log destination nv-file severity CRITICAL
log destination syslog 10.10.4.240 facility 7 severity DEBUG
no log engineering
log fields timestamp instance no-calling-task
no log here
```

```
Warning: Logging to this terminal is disabled
no log severity
```





















## CHAPTER 2

# Event Categories

This chapter lists each event category in the system software. To help you determine the severity level to set when troubleshooting, the log strategy for each event category is included. The log strategy shows the type of information logged for each severity level. In addition, this chapter includes the filters available in each event category.



## PART 2

# Event Categories

- [A Commands on page 25](#)
- [B Commands on page 35](#)
- [C Commands on page 51](#)
- [D Commands on page 57](#)
- [E Commands on page 79](#)
- [F Commands on page 81](#)
- [G and H Commands on page 87](#)
- [I Commands on page 91](#)
- [L Commands on page 129](#)
- [M Commands on page 145](#)
- [N Commands on page 165](#)
- [O Commands on page 169](#)
- [P Commands on page 193](#)
- [Q Commands on page 213](#)
- [R Commands on page 215](#)
- [S Commands on page 229](#)
- [T Commands on page 247](#)
- [U Commands on page 255](#)
- [V Commands on page 257](#)



## CHAPTER 3

# A Commands

- [aaaAtm1483Cfg on page 25](#)
- [aaaEngineGeneral on page 26](#)
- [aaaQosCfg on page 26](#)
- [aaaServerGeneral on page 27](#)
- [aaaUserAccess on page 28](#)
- [addressServerGeneral on page 28](#)
- [ar1AaaServerGeneral on page 29](#)
- [atm on page 29](#)
- [atm1483 on page 30](#)
- [atm1483VcClass on page 31](#)
- [atmAal5 on page 31](#)
- [atmVcClass on page 32](#)
- [auditIpsec on page 32](#)

### aaaAtm1483Cfg

---

<b>Description</b>	AAA ATM 1483 subinterface configuration
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Illegal service category traffic parameter received from AAA; unable to modify circuit traffic parameters using those received from AAA
<b>Notice Log</b>	None
<b>Info</b>	None









<b>Notice Log</b>	Interface pool expanded by an incremental number of entries; report retry delay in seconds when waiting for the underlying physical interface to be created; unable to allocate a message to send an interface up or down notification; unable to add or configure interface
<b>Info</b>	Dropping interface up, down, or not present notification due to removal of interface; discarding F4 OAM circuits when interface does not support F4 OAM
<b>Debug</b>	None
<b>Filter</b>	None

---

## atm1483

---

<b>Description</b>	ATM 1483 data service
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error applying static map entry for a newly created circuit of an NBMA interface; unable to configure interfaces on ATM interface; unable to determine interface location for ATM AAL5 interface; unable to determine maximum interface configuration count for interface; unable to configure interface on ATM interface
<b>Warning Log</b>	Error getting location of underlying AAL5 or ATM interface; error binding to AAL5 interface; error opening a circuit for an NBMA interface; attempting to associate a static map to an underlying ATM interface that does not exist; error restoring circuits from NVS; error removing static map entry; NVS entry not found for static map entry; error storing static map entry in NVS; error expanding interface pool, interface binding pool, or subscriber pool
<b>Notice Log</b>	Interface pool, interface binding pool, or subscriber pool expanded by an incremental number of entries; unable to allocate a message to send a subinterface up or down notification
<b>Info</b>	Dropping subinterface up or down notification due to removal of subinterface; configure interfaces on ATM interface; elapsed time for downloading interfaces; elapsed time for ATM AAL5 present notification; maximum interface count per call
<b>Debug</b>	None
<b>Filter</b>	None

## atm1483VcClass

---

<b>Description</b>	Application of attributes configured in a virtual circuit (VC) class to PVCs
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	In routers with high availability enabled, failure to mirror the VC modification or failure to associate the VC modification with the standby SRP module
<b>Warning Log</b>	Failure to find the PVCs associated with this VC class; failure to apply the VC class attributes to the appropriate PVCs; the log message displays a brief description of the failure
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## atmAal5

---

<b>Description</b>	ATM Adaptation Layer 5
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Error getting location of underlying ATM interface; error binding to ATM interface; unable to expand interface pool; error creating interface; unable to set administrative status of interface
<b>Notice Log</b>	Interface pool expanded by an incremental number of entries; report retry delay in seconds when waiting for the underlying ATM interface to be created; unable to allocate a message to send an interface up or down notification

<b>Info</b>	Dropping interface up or down notification due to removal of interface
<b>Debug</b>	None
<b>Filter</b>	None

---

## atmVcClass

---

<b>Description</b>	Information on VC class operational errors
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Resource failure errors, such as error allocating memory for adding a VC class; internal software errors; error processing a VC class association; when using SNMP, unable to set a VC class state from not in service to in service, or vice-versa; unable to find an existing VC class in the internal data structure; unable to complete processing after a high availability switchover
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Unable to update mirrored storage for a high availability switchover
<b>Filter</b>	None

---

## auditIpsec

---

<b>Description</b>	IKE SA negotiations
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None

**Notice Log** Information about IKE SA negotiation payloads

**Info** None

**Debug** None

**Filter** None



## CHAPTER 4

# B Commands

- [bfdAdaptivity](#) on page 35
- [bfdEvents](#) on page 36
- [bfdGeneral](#) on page 36
- [bfdSession](#) on page 37
- [bgpConnections](#) on page 37
- [bgpDampening](#) on page 38
- [bgpEvents](#) on page 39
- [bgpGeneral](#) on page 40
- [bgpGracefulRestart](#) on page 40
- [bgpIpv6Issu](#) on page 41
- [bgpIpv6NextHops](#) on page 42
- [bgpKeepAlives](#) on page 42
- [bgpMessages](#) on page 43
- [bgpNeighborChanges](#) on page 44
- [bgpNextHops](#) on page 45
- [bgpRoutes](#) on page 45
- [bridge](#) on page 48
- [bridgeEngine](#) on page 49
- [bridgingMgr](#) on page 49
- [bulkStats](#) on page 50

### [bfdAdaptivity](#)

---

**Description** BFD adaptivity events

**Emergency** None

**Alert** None

**Critical** None

<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	BFD session adaptivity events
<b>Debug</b>	BFD session adaptivity events
<b>Filter</b>	None

## **bfdEvents**

---

<b>Description</b>	BFD Events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	BFD session state changes
<b>Debug</b>	None
<b>Filter</b>	None

## **bfdGeneral**

---

<b>Description</b>	BFD general events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None

<b>Warning Log</b>	None
<b>Notice Log</b>	BFD enabled/disabled on an interface from a client
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## bfdSession

---

<b>Description</b>	BFD session events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Unknown BFD session
<b>Notice Log</b>	Session state changes
<b>Info</b>	Session parameter changes
<b>Debug</b>	None
<b>Filter</b>	None

## bgpConnections

---

<b>Description</b>	BGP TCP/IP connection activity
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error setting password for specified peer; error binding to update-source address for specified peer

<b>Warning Log</b>	TCP error occurred while receiving data
<b>Notice Log</b>	Outbound TCP connection initiated, completed, or failed; inbound TCP connection accepted, refused, or failed; TCP connection closed by peer
<b>Info</b>	None
<b>Debug</b>	TCP connection is ready to send; data received on TCP connection; notification message sent; could not send notification message due to flow control—will retry later; error while sending notification message; keepalive message sent; could not send keepalive message due to flow control—will retry later; error while sending keepalive message; message other than notification or keepalive sent; could not send other message than notification or keepalive due to flow control—will retry later; error while sending other message than notification or keepalive
<b>Filter 1</b>	access-class—This filter is not currently supported
<b>Filter 2</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3</b>	route-map—This filter is not currently supported
<b>Filter 4</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5</b>	in—This filter is not currently supported
<b>Filter 6</b>	out—This filter is not currently supported

---

## bgpDampening

---

<b>Description</b>	BGP dampening
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	Route is suppressed by route-flap dampening; route is no longer suppressed by route-flap dampening
<b>Info</b>	None

<b>Debug</b>	None
<b>Filter 1</b>	access-class—This filter is not currently supported
<b>Filter 2</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3</b>	route-map—This filter is not currently supported
<b>Filter 4</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5</b>	in—This filter is not currently supported
<b>Filter 6</b>	out—This filter is not currently supported

## bgpEvents

<b>Description</b>	BGP finite state machine (FSM) events and transitions
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Event occurred that was not expected for current state
<b>Warning Log</b>	None
<b>Notice Log</b>	One of the following events occurred: start, stop, inbound-connection-arrived, outbound-connection-complete, connection-error, connection-closed, start-timer-expired, connect-timer-expired, hold-timer-expired, keep-alive-timer-expired, open-received, update-received, keep-alive-received, notification-received, route-refresh, route-refresh-cisco
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter 1</b>	access-class—This filter is not currently supported
<b>Filter 2</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3</b>	route-map—This filter is not currently supported
<b>Filter 4</b>	router—See description of the bgpRoutes router filter for information about this filter

**Filter 5** in—This filter is not currently supported

**Filter 6** out—This filter is not currently supported

## bgpGeneral

---

<b>Description</b>	BGP general information
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	BGP IPv4 route-target-signaling address family enabled or disabled; making local route to multihomed site less preferred (local-preference < > ) because down bit is set
<b>Info</b>	None
<b>Debug</b>	Setting local preference to < > for redistributed route of layer2 site
<b>Filter 1</b>	access-class—This filter is not currently supported
<b>Filter 2</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3</b>	route-map—This filter is not currently supported
<b>Filter 4</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5</b>	in—This filter is not currently supported
<b>Filter 6</b>	out—This filter is not currently supported

## bgpGracefulRestart

---

<b>Description</b>	BGP Graceful Restart Feature log
<b>Emergency</b>	None
<b>Alert</b>	None

<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	Log BGP performed or did not perform a graceful restart; router supports or does not support non-stop forwarding; router is capable of switching gracefully, deferring, or resuming best path selection decision process; BGP routes allowed or prevented from being downloaded to line cards; graceful-restart timer expiration; marking or removing stale routes; waiting to receive end-of-rib marker from peer; received end-of-rib marker from all peers
<b>Info</b>	None
<b>Debug</b>	Standby SRP will wait for BGP convergence on next restart
<b>Filter 1</b>	access-class—This filter is not currently supported
<b>Filter 2</b>	peer—This filter is not currently supported
<b>Filter 3</b>	route-map—This filter is not currently supported
<b>Filter 4</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5</b>	in—This filter is not currently supported
<b>Filter 6</b>	out—This filter is not currently supported

## **bgplpv6Issu**

---

<b>Description</b>	BGP IPv6-specific information
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Notification disallowing any configuration
<b>Notice Log</b>	Notify the status of the unified ISSU signal

<b>Info</b>	None
<b>Debug</b>	Bind or unbind of the unified ISSU signal, keepalive, and graceful restart information
<b>Filter</b>	None

---

## bgpIpv6NextHops

---

<b>Description</b>	BGP indirect next-hops for IPv6 NLRI
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Errors in BGP IPv6 next hop events and state transitions
<b>Warning Log</b>	None
<b>Notice Log</b>	State transitions of BGP IPv6 next hops
<b>Info</b>	None
<b>Debug</b>	BGP IPv6 indirect next-hop events
<b>Filter 1</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 2</b>	remote-ipv6-address—Matches on the IPv6 address of the BGP indirect next-hop

---

## bgpKeepAlives

---

<b>Description</b>	BGP keepalive messages
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Keepalive message received with unexpected additional data after header
<b>Notice Log</b>	Keepalive message received; keepalive message sent

<b>Info</b>	None
<b>Debug</b>	None
<b>Filter 1</b>	access-class—This filter is not currently supported
<b>Filter 2</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3</b>	route-map—This filter is not currently supported
<b>Filter 4</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5</b>	in—Matches on traffic coming into the router
<b>Filter 6</b>	out—Matches on traffic going out of the router



**NOTE:** Send messages are logged to the bgpKeepAlives log when a message is added to the send queue. A debug message is logged in to the bgpConnections log when the message is actually passed to TCP.

## bgpMessages

<b>Description</b>	BGP protocol messages
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Unknown message type received; invalid field in received message; notification message received or sent; invalid capability length in received ORF capability; invalid capability value in received ORF capability; invalid ORF in received ORF capability; ORF entries exceeded maximum limit in received prefix list
<b>Notice Log</b>	Open message received or sent; update message received or sent; route-refresh message received or sent; route-refresh-cisco message received or sent; received ORF capability; received route refresh message with ORF entries
<b>Info</b>	None



**Filter 4** router—See description of the bgpRoutes router filter for information about this filter

**Filter 5** in—This filter is not currently supported

**Filter 6** out—This filter is not currently supported

## bgpNextHops

<b>Description</b>	VPN and non-VPN BGP indirect next hops
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Errors in BGP next hop events and state transitions
<b>Warning Log</b>	None
<b>Notice Log</b>	State transitions of BGP next hops
<b>Info</b>	None
<b>Debug</b>	BGP indirect next-hop events
<b>Filter 1</b>	access-class—This filter is not currently supported
<b>Filter 2</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3</b>	route-map—This filter is not currently supported
<b>Filter 4</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5</b>	in—Matches on traffic coming into the router
<b>Filter 6</b>	out—Matches on traffic going out of the router

## bgpRoutes

<b>Description</b>	BGP routing table updates
<b>Emergency</b>	None
<b>Alert</b>	None







<b>Info</b>	Bridge group state changes (start, shutdown); bridge interface, learning, aging, and static MAC address modifications
<b>Debug</b>	Verbose bridge interface, learning, aging, and static MAC address configuration and status
<b>Filter</b>	None

---

## bridgeEngine

---

<b>Description</b>	Bridge engine configuration
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Bridge engine, bridge agent, and bridge interface errors
<b>Warning Log</b>	Bridge engine resources (maximum interfaces, memory exhaustion)
<b>Notice Log</b>	Slot status; bridge interface location availability
<b>Info</b>	Bridge engine and bridge agent state changes (create, start, stop delete); bridge engine, bridge agent, and bridge interface modifications
<b>Debug</b>	Verbose bridge engine, bridge agent, and bridge interface configuration and status
<b>Filter</b>	None

---

## bridgingMgr

---

<b>Description</b>	Bridging manager configuration
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Bridge mode, bridge group, and subscriber policy errors
<b>Warning Log</b>	Bridging manager resources (maximum bridge groups, maximum subscriber policies, memory exhaustion)

<b>Notice Log</b>	None
<b>Info</b>	Bridging manager operation state changes (init, start, shutdown); bridge mode, bridge group, and subscriber policy modifications
<b>Debug</b>	Verbose bridge mode, bridge group, and subscriber policy configuration and status
<b>Filter</b>	None

---

## bulkStats

---

<b>Description</b>	Bulk statistics collector
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Operational failures, such as failed transfer—reverting to secondary receiver, file full, file creation failure, file deletion failure
<b>Notice Log</b>	File full or file nearly full conditions, preparing to send an SNMP trap
<b>Info</b>	Status of user configuration commands
<b>Debug</b>	Tracks performance progress of bulkstats application
<b>Filter</b>	None

## CHAPTER 5

# C Commands

- [cacGeneral](#) on page 51
- [cacIntf](#) on page 52
- [cliCommand](#) on page 52
- [cliGeneral](#) on page 53
- [connectionManager](#) on page 53
- [cops](#) on page 54
- [copsPr](#) on page 54
- [coreDump](#) on page 55
- [ctreeLog](#) on page 55

### [cacGeneral](#)

---

<b>Description</b>	CAC general purpose
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Unusual conditions in IGP/CAC interaction
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	General debugging info
<b>Filter</b>	None

## cacIntf

---

<b>Description</b>	CAC interface events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Unusual or failure situations in interface processing
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Interface level debugging info
<b>Filter</b>	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"><li>• <i>interface</i>—Logs events for a specific interface</li><li>• <i>interfaceType</i>—Type of interface on which you want to log events</li><li>• <i>interfaceSpecifier</i>—Location of interface in the appropriate format</li></ul>



**NOTE:** For information about interface types and specifiers, see Interface Types and Specifiers in *JunosE Command Reference Guide*.

---

## cliCommand

---

<b>Description</b>	CLI commands
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None

<b>Notice Log</b>	All successful CLI configuration commands
<b>Info</b>	All unsuccessful CLI configuration commands; all nonconfiguration commands
<b>Debug</b>	None
<b>Filter</b>	None

## cliGeneral

---

<b>Description</b>	CLI general log
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	CLI command mode from prior release no longer exists; the overridden privilege level command will be discarded
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## connectionManager

---

<b>Description</b>	Logging various conditions in the component that manages the chassis fabric.
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	10G and 5G SRP modules only—Detection that the FPGAs have not been loaded (results in an SRP [and chassis] reset)
<b>Error</b>	10G and 5G SRP modules only—That there is not enough bandwidth for a particular board in the system, that connections could not be added in the fabric due to resource limitations (such as memory), that a board was just removed and the resource will not

be needed when this condition is detected momentarily, or that a connection cannot be closed or a multicast destination cannot be dropped.

<b>Warning Log</b>	Cannot connect to a particular source or destination address (board may have just been removed)
<b>Notice Log</b>	A connection that previously could not be closed has now closed; a multicast destination that previously could not be dropped has now been dropped
<b>Info</b>	Various logs to indicate events and transitions for low level diagnosis
<b>Debug</b>	Various logs to indicate events and transitions for low level diagnosis
<b>Filter</b>	None

---

## cops

<b>Description</b>	Common Open Policy Service (COPS) protocol
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	COPS message with bad header, version, length, or client
<b>Warning Log</b>	Unexpected socket event
<b>Notice Log</b>	COPS layer enabled or disabled; socket remotely closed
<b>Info</b>	None
<b>Debug</b>	COPS session instantiation or removal; COPS connection or socket creation or deletion; keepalive value
<b>Filter</b>	None

---

## copsPr

<b>Description</b>	COPS-PR general log
<b>Emergency</b>	None
<b>Alert</b>	None

<b>Critical</b>	None
<b>Error</b>	Error decoding COPS-PR messages received from the SDX program
<b>Warning Log</b>	Outstanding COPS-PR pool allocations while attempting to shut down SSC client; temporary resource allocations while sending COPS-PR messages to SDX program
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## coreDump

---

<b>Description</b>	Core dump events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Connection errors; file open errors; write failures; core dump failures; transfer errors
<b>Warning Log</b>	Core dump configuration changes due to core dump monitor; core dump monitor memory allocation errors
<b>Notice Log</b>	Successful line card core dump; core dump attempts; core dump progression; core dump monitor checks; core dump monitor transfer completions; core dump monitor dump file deletion
<b>Info</b>	None
<b>Debug</b>	lcLoader creation; dump request receipt; core dump monitor start; core dump monitor stop
<b>Filter</b>	None

## ctreeLog

---

<b>Description</b>	For internal maintenance of IP routes
<b>Emergency</b>	None

<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Failure in insertion, deletion, and update of IP routes in internal data structure used to maintain the routes
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Creation or deletion of an internal data structure
<b>Filter</b>	None

## CHAPTER 6

# D Commands

- [dcm](#) on page 58
- [dcmEngineGeneral](#) on page 58
- [debounceEvents](#) on page 59
- [debounceGeneral](#) on page 59
- [dhcpCapture](#) on page 60
- [dhcpExternal](#) on page 60
- [dhcpExternalEngine](#) on page 61
- [dhcpGeneral](#) on page 61
- [dhcplssuLog](#) on page 62
- [dhcpLocalClients](#) on page 62
- [dhcpLocalGeneral](#) on page 63
- [dhcpLocalHighAvailability](#) on page 63
- [dhcpLocalPool](#) on page 64
- [dhcpLocalProtocol](#) on page 64
- [dhcpOfferLog](#) on page 65
- [dhcpPbeGeneral](#) on page 66
- [dhcpProxyGeneral](#) on page 66
- [dhcpRelayGeneral](#) on page 67
- [dhcpRelayNvWriterGeneral](#) on page 67
- [dhcipv6Client](#) on page 68
- [dhcipv6DemuxGeneral](#) on page 68
- [dhcipv6LocalSubInterfaceTable](#) on page 69
- [dhcipv6LsGeneral](#) on page 69
- [dismanEventManager](#) on page 70
- [dnsGeneralLog](#) on page 71
- [dosProtection](#) on page 71
- [ds1](#) on page 72
- [ds3](#) on page 72

- [dvmrpGeneral](#) on page 73
- [dvmrpGracefulRestart](#) on page 74
- [dvmrpMcastTable](#) on page 74
- [dvmrpProbeRcv](#) on page 75
- [dvmrpProbeSent](#) on page 75
- [dvmrpRtTable](#) on page 76

---

## dcm

<b>Description</b>	Dynamic Configuration Manager
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Schedule engine event; status of dynamic interface creation; receipt of teardown signal for a dynamic interface; no interface adapter to propagate teardown; creation of dynamic PPP interface failed; creation of dynamic PPPoE interface failed
<b>Filter</b>	None

---

## dcmEngineGeneral

<b>Description</b>	DCM engine general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None

<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Giving notify credits to line module; receipt of request buffer from line module; starting line module communication session; Ack/Nack dynamic interface creation request
<b>Filter</b>	None

## debounceEvents

---

<b>Description</b>	Events causing changes to the upper-layer link status based on Ethernet debounce configuration
<b>Emergency</b>	None
<b>Alert</b>	Debounce preempted; link stabilized to operational up or down status
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	Events causing finite state machine transitions
<b>Info</b>	Events not causing finite state machine transitions
<b>Debug</b>	None
<b>Filter</b>	None

## debounceGeneral

---

<b>Description</b>	Ethernet debounce configuration status log
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error in enabling or disabling the debounce timer on the Ethernet interface
<b>Warning Log</b>	None



<b>Notice Log</b>	Configuration changes
<b>Info</b>	None
<b>Debug</b>	Configuration change details; client events
<b>Filter</b>	None

---

## dhcpExternalEngine

---

<b>Description</b>	DHCP external engine
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Configuration errors; client processing errors (invalid data)
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	System events (line cards online/offline)
<b>Debug</b>	Configuration change details; client events
<b>Filter</b>	None

---

## dhcpGeneral

---

<b>Description</b>	DHCP general
<b>Emergency</b>	None
<b>Alert</b>	Rvn8
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None

<b>Info</b>	None
<b>Debug</b>	DHCP message received
<b>Filter</b>	None

---

## dhcpIssuLog

---

<b>Description</b>	DHCP ISSU information
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error recreating DHCP ISSU IC shadow and its data structures, followed by an ISSU halt
<b>Warning Log</b>	Buffering capacity exceeded between DHCP engine and the driver/ISSU shadow driver
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Normal operation: packet processing events, creation and deletion of DHCP common objects during ISSU
<b>Filter</b>	None

---

## dhcpLocalClients

---

<b>Description</b>	DHCP local server clients
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Cannot find the client's interface; cannot find the client to expire the lease or remove it from the database; trying to expire client's lease or remove it from database with bad IP address; requested MAC address does not match the available address; cannot allocate SDX subscriber information
<b>Warning Log</b>	Cannot find the DHCP instance for the client with an expired lease; cannot find the DHCP instance to release the client IP address; secondary DNS without primary DNS configured,



<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Out of resources errors; nonrecoverable software errors during client restoration or mirroring, pool creation/modification; recoverable software errors during modification of existing client
<b>Warning Log</b>	Recoverable software errors during client, server or pool configuration; out of resources on new client, server, or pool configuration; timer configuration problems
<b>Notice Log</b>	Normal recovery following SRP switch
<b>Info</b>	None
<b>Debug</b>	Normal client, server, pool processing
<b>Filter</b>	None

---

## dhcpLocalPool

---

<b>Description</b>	DHCP local address pool, including normal, linked, and shared pools
<b>Emergency</b>	None
<b>Alert</b>	Local pool IP address is exhausted (address limit violation)
<b>Critical</b>	Higher limit of address pool utilization reached
<b>Error</b>	None
<b>Warning Log</b>	Lower limit of address pool utilization reached; invalid DHCP local address pool attributes
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	DHCP local address pool resolution; address allocation; minimum or maximum threshold values are modified for the base pool in a linked pool
<b>Filter</b>	None

---

## dhcpLocalProtocol

---

<b>Description</b>	DHCP local server protocol
--------------------	----------------------------

<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Cannot find interface; remote client bind add failed; client failed to decline IP address; client failed to decline a null offered IP address; delete remote client entry failed
<b>Warning Log</b>	AAA not responding; SDX program not responding; rediscovering with no IP address allocated; a renewal is received on the line module for an unknown client; secondary DNS without primary DNS configured, using DHCP values; secondary NetBIOS Name Server (NBNS) without primary NBNS configured, using DHCP values; duplicate MAC address detected
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Received packet; transmit packet; authentication status; DHCP local server state transitions
<b>Filter</b>	<p>interface <i>interfaceType interfaceSpecifier</i></p> <ul style="list-style-type: none"> <li>• <i>interface</i>—Logs events for a specific interface</li> <li>• <i>interfaceType</i>—Type of interface for which you want to log events</li> <li>• <i>interfaceSpecifier</i>—Location of interface in the appropriate format</li> </ul>



**NOTE:** For information about interface types and specifiers, see *Interface Types and Specifiers* in *JunosE Command Reference Guide*.

## dhcpOfferLog

<b>Description</b>	DHCP offer selection process log
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None

<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Status of the offer selection process
<b>Filter</b>	None

---

## dhcpPbeGeneral

---

<b>Description</b>	DHCP Proxy Backend Log
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Heap exhaustion
<b>Warning Log</b>	Failure to send a DHCP message to a client
<b>Notice Log</b>	Failure to restore client after reboot or interface change; failure to allocate memory from task-controlled pools
<b>Info</b>	None
<b>Debug</b>	Status of task and DHCP operations
<b>Filter</b>	None

---

## dhcpProxyGeneral

---

<b>Description</b>	DHCP Proxy general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None

<b>Warning Log</b>	None
<b>Notice Log</b>	Cold and warm restart of DHCP proxy client; DHCP proxy client starts and ends the restoration of client bindings from the mirrored storage for a virtual router
<b>Info</b>	None
<b>Debug</b>	Control flow and key events; DHCP proxy client ends the process of restoring client bindings on a virtual router; DHCP proxy client restores each client binding from mirrored storage with the client IP address and state of the binding
<b>Filter</b>	None

### **dhcpRelayGeneral**

---

<b>Description</b>	DHCP Relay general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	Warm start recovery problems (high availability and unified ISSU)
<b>Info</b>	None
<b>Debug</b>	Control flow and key events, packets that are transmitted using the layer 2 unicast feature, status and changes to DHCP relay agent information option and suboptions
<b>Filter</b>	None

### **dhcpRelayNvWriterGeneral**

---

<b>Description</b>	DHCP host route preservation
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None

<b>Error</b>	Out of memory conditions
<b>Warning Log</b>	Unexpected unified ISSU signal, removing all NVS and routing table entries at startup, removing routing table entries at startup due to inconsistencies
<b>Notice Log</b>	Removing or adding entries on start up due to inconsistencies
<b>Info</b>	None
<b>Debug</b>	Receiving unified ISSU signal, construction of the writer, saving to NVS, removing router, removing routes, adding routes
<b>Filter</b>	None

---

## dhcpv6Client

---

<b>Description</b>	DHCPv6 internal test client events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Problems communicating with IPv6; invalid message types received; out-of-memory conditions; serious DHCPv6 protocol state errors; internal errors
<b>Warning Log</b>	Minor DHCPv6 protocol errors
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

---

## dhcpv6DemuxGeneral

---

<b>Description</b>	DHCPv6 packet demultiplexer events
<b>Emergency</b>	None
<b>Alert</b>	None



<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Failure to create server (bad router or out of memory); errors encountered while processing ISSU signals or while mirroring; initialization error during the configuration of the DUID type
<b>Warning Log</b>	Attempt to remove a nonexistent server; any failure during the configuration of the DUID type
<b>Notice Log</b>	Failure to create server (IPv6 not licensed); cold/warm restart of DHCPv6 local server; before/after restoring client bindings; warm SRP switchover problems during the configuration of the DUID type
<b>Info</b>	None
<b>Debug</b>	Server bind, creation, deletion, unbind, and restoration of bindings post warm SRP switchover; Prefix Allocation Notification: designated prefix is already in use by another client; if ISSU is running on a DHCPv6 local server, ISSU and HA debug messages are logged; authentication of subscribers with the AAA username
<b>Filter</b>	None

---

## dismanEventMgr

---

<b>Description</b>	Distributed management event manager
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Configuration errors; Sampling, testing and setting errors
<b>Warning Log</b>	Limit maximums reached
<b>Notice Log</b>	Trigger values reached
<b>Info</b>	Application started; traps activated; sampling information provided
<b>Debug</b>	None
<b>Filter</b>	None

## dnsGeneralLog

---

<b>Description</b>	DNS general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Failure to post a message to DNS about the query response from DNS server
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Dump DNS response packet; trace DNS query submission; trace DNS response parsing and processing; trace dropped queries if router is shutting down or DNS disabled in virtual router; trace DNS cache cleanup
<b>Filter</b>	None

## dosProtection

---

<b>Description</b>	DoS general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Suspicious control flows exceed threshold for specific line module; possible distributed DoS attack
<b>Error</b>	Control flow changed to suspicious.
<b>Warning Log</b>	Flow table overflow, protocol (or priority) has transitioned to suspicious
<b>Notice Log</b>	Suspicious control flow returned to nonsuspicious protocol (or priority) has transitioned from suspicious
<b>Info</b>	Suspicious control flow deleted
<b>Debug</b>	None











**Filter 2** router—See description of the `dvmpGeneral` router filter for information about this filter



## CHAPTER 7

# E Commands

- [ethernet](#) on page 79
- [ethernetStateSession](#) on page 79

### ethernet

---

<b>Description</b>	Ethernet layer
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Cannot configure Ethernet interface successfully; memory pool depleted
<b>Notice Log</b>	No pool space; can bring interface up
<b>Info</b>	Hardware present or not present notification
<b>Debug</b>	Interface created or deleted
<b>Filter</b>	None

### ethernetStateSession

---

<b>Description</b>	Configuration of the Fast Ethernet management port on the SRP IOA on the E320 router or the E120 router
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None

<b>Error</b>	Configuration errors for duplex mode and speed settings on the Fast Ethernet management port
<b>Warning Log</b>	Configuration did not occur for duplex mode and speed on the Fast Ethernet management port
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## CHAPTER 8

# F Commands

- [fileSystem](#) on page 81
- [flowInspection](#) on page 82
- [flowInspectionEngine](#) on page 82
- [flowServicesFirewallAlert](#) on page 83
- [flowServicesFirewallAudit](#) on page 83
- [frameRelay](#) on page 84
- [fsAgent](#) on page 84
- [ftl](#) on page 85
- [ftpClient](#) on page 85
- [ftpServer](#) on page 86

### fileSystem

---

<b>Description</b>	File system
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Configuration consistency check failed; HA/sync may be disabled
<b>Error</b>	Error enabling or disabling
<b>Warning Log</b>	Missing of invalid armed files
<b>Notice Log</b>	Configuration checker enabled or disabled
<b>Info</b>	None
<b>Debug</b>	Timestamp of last synchronization
<b>Filter</b>	None

## flowInspection

---

<b>Description</b>	Flow inspection
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Configuration error for bulk static translations; failure to increase size of translation database; pool range overlap; more DNS queries than can be processed
<b>Warning Log</b>	Translation timeout change not applied to existing translations; failure to install translations
<b>Notice Log</b>	None
<b>Info</b>	Allocation and deallocation of NAT address or NAPT address/port
<b>Debug</b>	Increase size of translation database; add or remove address pool ranges
<b>Filter</b>	None

## flowInspectionEngine

---

<b>Description</b>	Flow inspection engine
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Virtual router not found during deletion request
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Engine creation, timer state information, setCoreLocation notification
<b>Filter</b>	None

## flowServicesFirewallAlert

---

<b>Description</b>	Firewall
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	No resources; number of connections has exceeded the specified limit; destination host is blocked or cleared; NAT disallows a connection; no controlling list; bad packet received
<b>Warning Log</b>	None
<b>Notice Log</b>	Oldest entry deleted; rate of connections has decreased to the specified limit; number of connections has decreased to below the specified limit
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## flowServicesFirewallAudit

---

<b>Description</b>	Firewall
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	New connection disallowed
<b>Warning Log</b>	None
<b>Notice Log</b>	Transition from half-open to fully complete connection; transition to half-open connection
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## frameRelay

---

<b>Description</b>	Frame Relay layer
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Failure to bring up the application due to lack of memory resources
<b>Error</b>	Summary information about automatic removal of interface or circuit from nonvolatile storage on startup; internal resource pool is too small
<b>Warning Log</b>	None
<b>Notice Log</b>	Lack of pool space for SNMP traps (it is permissible for SNMP traps to be unreliable); failure to obtain line module configuration on line module insertion
<b>Info</b>	Line module insertion and removal information
<b>Debug</b>	Creation of interfaces or circuits from nonvolatile storage on startup; detailed information about automatic removal of interfaces or circuit from nonvolatile storage on startup; reporting on SNMP traps for interfaces or circuits; engine debug messages
<b>Filter</b>	None

## fsAgent

---

<b>Description</b>	File System Agent
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Previous file system sync failed—booting protected images
<b>Error</b>	File system unavailable
<b>Warning Log</b>	File transfer initialization failure; unexpected software error
<b>Notice Log</b>	None
<b>Info</b>	File transfer notification; platform or release mismatch; file transfer error; release file is corrupt; image path not found; insufficient resources to copy release



<b>Info</b>	Completion status of a user command (example: "IS command succeeded" )
<b>Debug</b>	None
<b>Filter</b>	None

---

## ftpServer

---

<b>Description</b>	FTP server
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error listening for new client connection; error creating daemon task
<b>Warning Log</b>	Error creating new server task; socket write error; error adjusting socket window size
<b>Notice Log</b>	Daemon task created; waiting for new client connection; accept client from host a.b.c.d; maximum client sessions exceeded; FTP daemon shutdown complete
<b>Info</b>	Starting FTP daemon shutdown
<b>Debug</b>	Read FTP command
<b>Filter</b>	None







- Info** Start or stop HTTP process; create or remove httpd; growing a pool of httpds; enable or disable httpd; growing a pool of HTTP connections (https); failure to perform TCP socket accept; growing a pool of HTTP events; updated HTTP scalars; handed out (global/token) address to dhcp-ls client; authentication passed from dhcp-ls for a given client; renewing token address for dhcp-ls client; removed session with dhcp-ls; removed global address through gplaanDelete; dhcp-ls user login/logout/shortcut login; create or remove HTTP interface redirect URL
- Debug** Server self-bind (for example, started HTTP without instantiating any httpd); attempt to remove nonexistent httpd; attempt to reread from NVS; updated httpd; create or remove session with dhcp-ls; bind or unbind with policy table; invalid or valid TCP socket approve or accept; received data from stale socket; create or remove HTTP connection; receive data from httpc; queued HTTP event; aging group of https; added new address at dhcp-ls session; phase 1 of 2 for authentication passed from dhcp-ls for a given client; revoking token address for a given dhcp-ls client
- Filter** None









































































<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	IPSec transport protocol interaction failures; interface engine interaction failures; IPSec transport profile configuration errors; interface configuration errors
<b>Warning Log</b>	Recoverable IPSec transport interface–related configuration and operational error
<b>Notice Log</b>	IPSec transport interface state change
<b>Info</b>	IPSec transport interface interaction with IKE protocol; interface pool usage
<b>Debug</b>	Details about the interaction between the IPSec transport interface and the IKE protocol; configuration and operational changes of the IPSec transport interface events; interface engine interaction
<b>Filter</b>	None

































<b>Critical</b>	None
<b>Error</b>	Unknown algorithm for local password
<b>Warning Log</b>	Connection granted or denied due to possible misconfiguration
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Connection granted or denied due to incorrect password
<b>Filter</b>	None







































































































































- **interface**—Logs PPP events for a specific interface
- **interfaceType**—Type of interface for which you want to log PPP events. For example, atm or fastEthernet
- **interfaceSpecifier**—Location of interface in the appropriate format



.....

**NOTE:** For information about interface types and specifiers, see *Interface Types and Specifiers* in *JunosE Command Reference Guide*.

.....

---

## profileMgr

<b>Description</b>	Profile manager
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Profile manager process creation failed
<b>Warning Log</b>	Profile being removed was not found
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Initialize profiles from NVS at startup; dump list of profiles after startup initialization; read or save profile numbering seed to and from NVS; profile manager process creation succeeded; NVS updated; profile lookup succeeded; validating or executing removal of profile
<b>Filter</b>	None

## CHAPTER 16

# Q Commands

- [qm on page 213](#)
- [qos on page 213](#)
- [qosAttachment on page 214](#)

### qm

---

<b>Description</b>	Queue manager
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Queue memory errors; line module queue errors; queue database synchronization errors
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

### qos

---

<b>Description</b>	QoS events
<b>Emergency</b>	None
<b>Alert</b>	None

<b>Critical</b>	None
<b>Error</b>	QoS object creation and modification failures due to resource limitations or configuration limitations; QoS profile to interface attachment failures; QoS failover messages reported by line module
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	Modification, creation, and destruction of QoS objects; attachment of modification of QoS objects; attachment of QoS profiles to interfaces; detachment of QoS profiles from interfaces; modification of QoS profiles; QoS interface location availability operations
<b>Debug</b>	Dynamic attachment of QoS profile to interfaces
<b>Filter</b>	None

---

## qosAttachment

---

<b>Description</b>	QoS profile attachment to interface configuration
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	QoS attachment failures
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	Attachment of QoS profiles; modification of QoS profile attachments
<b>Debug</b>	Dynamic attachment of QoS profiles; QoS profile attach/detach tracing
<b>Filter</b>	None





<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Displays CoA requests and replies received by the router, including the attributes; reports changes to the Service-Acct-Interval attribute (Juniper VSA 26-140); Agent Circuit ID, Agent Remote ID (DSL Forum VSA) and DHCP Option 82
<b>Filter</b>	None

### **radiusDisconnectGeneral**

---

<b>Description</b>	RADIUS Disconnect and CoA General
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	CoA failures resulting from memory allocation failures
<b>Debug</b>	CoA results received that do not match pending CoA requests
<b>Filter</b>	None

### **radiusRelayGeneral**

---

<b>Description</b>	RADIUS Relay Server general
--------------------	-----------------------------





<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Rising trap
<b>Notice Log</b>	Falling trap
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

---

## ripBfd

---

<b>Description</b>	RIP and BFD interaction and RIP session log
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Client session creation, update, and deletion failures
<b>Warning Log</b>	unknown RIP peer
<b>Notice Log</b>	None
<b>Info</b>	BFD session state changes
<b>Debug</b>	None
<b>Filter</b>	Router and interface

---

## ripGeneral

---

<b>Description</b>	RIP system notifications
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None







## rsvpAsyncMgr

---

<b>Description</b>	RSVP asynchronous manager events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Events processed by the asynchronous manager (for example, qos-profile/policy creation/deletion/attachment)
<b>Filter</b>	None

## rsvpBfd

---

<b>Description</b>	RSVP-TE and BFD interaction
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	RSVP-TE client session create failed
<b>Notice Log</b>	None
<b>Info</b>	BFD session create failed for IP address
<b>Debug</b>	Delete BFD; RSVP-TE established session with BFD manager; Creating BFD session for interface; deleting BFD session for interface
<b>Filter</b>	Router and interface





**Error** Operational errors; resource allocation failures

**Warning Log** Operational failures; fast-reroute triggering

**Notice Log** Less serious operational failures; network changes

**Info** Minor internal errors; timer operations

**Debug** Function flows, parameter passing

**Filter** router *virtualRouterName*

- router—Logs events for traffic on a specific virtual router
- *virtualRouterName*—Name of virtual router



## CHAPTER 18

# S Commands

- [security](#) on page 230
- [serviceability](#) on page 230
- [serviceMgr](#) on page 231
- [serviceMgrClientSession](#) on page 231
- [serviceMgrDcm](#) on page 232
- [serviceMgrMacroManager](#) on page 232
- [serviceMgrPerformance](#) on page 233
- [serviceMgrServiceDef](#) on page 233
- [serviceMgrServiceInstance](#) on page 234
- [serviceMgrServiceSession](#) on page 234
- [serviceMgrSubscriberSession](#) on page 235
- [sftpClient](#) on page 235
- [slep](#) on page 236
- [snmp](#) on page 236
- [snmplfMib](#) on page 237
- [snmpPduAudit](#) on page 237
- [snmpSetPduAudit](#) on page 238
- [snmpTrap](#) on page 238
- [sonet](#) on page 239
- [sonetPath](#) on page 239
- [sonetVT](#) on page 240
- [ssccDetailPm](#) on page 240
- [ssccDetailSsc](#) on page 241
- [ssccGeneral](#) on page 241
- [ssccLacGeneral](#) on page 242
- [ssh](#) on page 242
- [stTunnel](#) on page 243

- [stTunnelEngine](#) on page 244
- [system](#) on page 244

## security

---

<b>Description</b>	CLI security messages
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Suspected denial of service attack
<b>Error</b>	None
<b>Warning Log</b>	Unrecognized username, invalid password, denied host
<b>Notice Log</b>	User connect, user disconnect
<b>Info</b>	vty allocation success and failure, vty disconnect.
<b>Debug</b>	None
<b>Filter</b>	None

## serviceability

---

<b>Description</b>	Log for serviceability features (currently only for the <b>show tech-support</b> command)
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Insufficient memory to complete the command
<b>Warning Log</b>	The file to support this command is invalid
<b>Notice Log</b>	Normal milestones of command completion
<b>Info</b>	Timing information of <b>show tech-support</b> command
<b>Debug</b>	Detailed information of <b>show tech-support</b> command progress
<b>Filter</b>	None

---

## serviceMgr

---

<b>Description</b>	Service manager
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

---

## serviceMgrClientSession

---

<b>Description</b>	Service manager client session
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## serviceMgrDcm

---

<b>Description</b>	Service manager DCM
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## serviceMgrMacroManager

---

<b>Description</b>	Service manager macro manager
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## serviceMgrPerformance

---

<b>Description</b>	Service manager performance
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## serviceMgrServiceDef

---

<b>Description</b>	Service manager definition
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## serviceMgrServiceInstance

---

<b>Description</b>	Service manager service instance
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## serviceMgrServiceSession

---

<b>Description</b>	Service manager service session
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## serviceMgrSubscriberSession

---

<b>Description</b>	Service manager subscriber session
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Information about detected abnormalities during execution
<b>Warning Log</b>	Information about exceeded thresholds
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Information about the code path executed along with values of parameters
<b>Filter</b>	None

## sftpClient

---

<b>Description</b>	SFTP client log details
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Errors generated during the establishment of a new SFTP session; errors that are returned by the SFTP server
<b>Warning Log</b>	Socket read error
<b>Notice Log</b>	None
<b>Info</b>	Encryption algorithms supported; connection to the SFTP server port is established
<b>Debug</b>	Response received from the SFTP server
<b>Filter</b>	None

## step

---

<b>Description</b>	Point-to-Point Protocol layer
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Startup interface out of resources failure
<b>Error</b>	Remove or unbind interface failure; unknown or missing lower binding failure
<b>Warning Log</b>	Attempt to set characteristics with invalid value
<b>Notice Log</b>	None
<b>Info</b>	Hardware state change notification
<b>Debug</b>	None
<b>Filter</b>	<i>serial interfaceSpecifier</i> <ul style="list-style-type: none"><li>• <i>serial</i>—Logs SLEP events for a specific serial Cisco-HDLC interface</li><li>• <i>interfaceSpecifier</i>—Identifier for a serial Cisco-HDLC interface</li></ul>



.....  
**NOTE:** For information about interface types and specifiers, see *Interface Types and Specifiers* in *JunosE Command Reference Guide*.  
.....

## snmp

---

<b>Description</b>	Embedded SNMP agent
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Access violation due to underprivileged community string or a bad proxy selector; access denial due to configured access list; configuration of SNMP failed; trap is dropped because of the severity level filter or because the trap category is not enabled

<b>Notice Log</b>	None
<b>Info</b>	SNMP agent has been enabled or disabled
<b>Debug</b>	Trap request dropped; trap processing summary statistics
<b>Filter</b>	None

## snmpIfMib

---

<b>Description</b>	SNMP Interfaces MIB
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Invalid ifTableLastChange reported by an interface
<b>Warning Log</b>	Failed to process an interface for ifNumber MIB attribute computation
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

## snmpPduAudit

---

<b>Description</b>	SNMP PDUs
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None

<b>Info</b>	Identifies the following fields in all SNMP PDUs sent to the E Series router and all trap PDUs that leave the system: source and destination IP address, PDU type, snmpVersion, requested, errorStatus, errorIndex, variable count, variable object identifier and data
<b>Debug</b>	None
<b>Filter</b>	None

---

## snmpSetPduAudit

---

<b>Description</b>	SNMP set PDUs
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	Identifies the following fields in SNMP set PDUs: source and destination IP address, PDU type, snmpVersion, requested, errorStatus, errorIndex, variable count, variable object identifier and data
<b>Debug</b>	None
<b>Filter</b>	None

---

## snmpTrap

---

<b>Description</b>	SNMP Trap PDU events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	TX Power High Warning; TX Power Low Warning; RX Power High Warning; RX Power Low Warning

<b>Notice Log</b>	None
<b>Info</b>	SNMP trap PDUs that the corresponding SNMP agent transmitted
<b>Debug</b>	None
<b>Filter</b>	None

## sonet

<b>Description</b>	SONET
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Configuration errors, NVS failures
<b>Warning Log</b>	NV interface removal after failed init from NV; errors during interface add/update or during hwPresent notification; path capability notification; failed pool expansion
<b>Notice Log</b>	Pool expansion, dropped SNMP traps
<b>Info</b>	NV interface creation; interface modification from path capability; unknown interface during hwNotPresent notification; interface notification for unknown interface
<b>Debug</b>	Application initialization trace, interface creation/deletion events
<b>Filter</b>	None

## sonetPath

<b>Description</b>	SONET Path
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None











out of synchronization notification; NVS subsystem redundancy size mismatch; line module ID block misconfigured

**Notice Log** Subsystem failure condition abatement (heap/CPU utilization, NVS, power, fan, network timing, temperature); new module announcement; module revision mismatch; module upgraded or downgraded (ECC/non-ECC); module online or offline

**Info** Synchronization start, complete; line module set timing failed (not necessarily an error); NVS volume flush

**Debug** Module state change; module memory announcement; redundancy role changes; server role changes; module enable, disable, or clear notification; file system synchronization (normal operation); line module timing source set failure (not necessarily an error); image protection notification

**Filter** slot *slotNumber*

- slot—Logs events for a specific slot
- *slotNumber*—Number of slot for which you want to log events



## CHAPTER 19

# T Commands

- [tacacsPlusServer](#) on page 247
- [tcpGeneral](#) on page 248
- [tcpTraffic](#) on page 248
- [tcpv6Traffic](#) on page 249
- [telnet](#) on page 250
- [telnetClient](#) on page 250
- [tftpClient](#) on page 251
- [trackerEvents](#) on page 251
- [trackerGeneral](#) on page 252
- [tsm](#) on page 252

### **tacacsPlusServer**

---

<b>Description</b>	TACACS+ server
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Unable to start TACACS+; failed to create tacacsPlusProcess instance while in startup
<b>Warning Log</b>	Failed to create a host while reading parameters from NVS; primary host not found in NVS; more than one primary host found in NVS; number of primary hosts in NVS is not one, and attempts to correct this condition failed; unable to bind socket to source address configured to TACACS+ server
<b>Notice Log</b>	Received unexpected data from the TACACS+ host, which will result in authentication failure; either there is no host in NVS, or all attempts to configure a host failed
<b>Info</b>	None



<b>Notice Log</b>	TCP packet discards due to MD5 authorization failure and checksum failure
<b>Info</b>	None
<b>Debug</b>	Report all TCP receive and transmit events; Records the retry option or message
<b>Filter 1</b>	remote-ip-address <i>ipAddress</i> [ <i>ipAddressMask</i> ] <ul style="list-style-type: none"> <li>• remote-ip-address—Logs events for a remote address</li> <li>• <i>ipAddress</i>—Address of remote system for which you want to log messages</li> <li>• <i>ipAddressMask</i>—Mask for the remote address</li> </ul>
<b>Filter 2</b>	router <i>virtualRouterName</i> [ remote-ip-address <i>ipAddress</i> [ <i>ipAddressMask</i> ] ] <ul style="list-style-type: none"> <li>• router—Logs events on a specific virtual router</li> <li>• <i>virtualRouterName</i>—Name of virtual router for which you want to log events</li> <li>• remote-ip-address—Logs events for a remote address</li> <li>• <i>ipAddress</i>—Address of remote system for which you want to log messages</li> <li>• <i>ipAddressMask</i>—Mask for the remote address</li> </ul>

## tcpv6Traffic

<b>Description</b>	TCP frame transmit and receive
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	TCP packet discards due to MD5 authorization failure and checksum failure
<b>Info</b>	None
<b>Debug</b>	Report all TCP receive and transmit events
<b>Filter 1</b>	remote-ip-address <i>ipAddress</i> [ <i>ipAddressMask</i> ] <ul style="list-style-type: none"> <li>• remote-ip-address—Logs events for a remote address</li> <li>• <i>ipAddress</i>—Address of remote system for which you want to log messages</li> </ul>

- *ipAddressMask*—Mask for the remote address

**Filter 2** `router virtualRouterName [ remote-ip-address ipAddress [ ipAddressMask ] ]`

- *router*—Logs events on a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events
- *remote-ip-address*—Logs events for a remote address
- *ipAddress*—Address of remote system for which you want to log messages
- *ipAddressMask*—Mask for the remote address

---

## telnet

<b>Description</b>	Telnet daemon
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error condition binding to or listening on Telnet sockets; unexpected software error; NVS mismatch; insufficient memory resources
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Stopped listening on a specified router
<b>Filter</b>	None

---

## telnetClient

<b>Description</b>	Telnet client log
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None

<b>Warning Log</b>	None
<b>Notice Log</b>	Unexpected socket condition; unable to connect to remote host; successful connection; ENV send failure; resource allocation failure
<b>Info</b>	Connection attempt; detailed connection information (per connection); escape character announcement; connection closed
<b>Debug</b>	None
<b>Filter</b>	None

## tftpClient

---

<b>Description</b>	TFTP client log
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Memory allocation failures
<b>Warning Log</b>	None
<b>Notice Log</b>	TFTP error message received from remote host
<b>Info</b>	Initiating communication with remote host; discarded messages
<b>Debug</b>	TFTP responses received from incorrect source port on remote host
<b>Filter</b>	None

## trackerEvents

---

<b>Description</b>	Tracker event propagation
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None



<b>Warning Log</b>	Nonvolatile storage integrity problems; memory exhaustion-based denial of service; number of interfaces in use reaching high levels
<b>Notice Log</b>	Nonvolatile storage allocation problems; memory pool expansion
<b>Info</b>	Resource-restriction based denial of service; line module up or down transitions
<b>Debug</b>	Program debugging information including function call tracing
<b>Filter</b>	None



## CHAPTER 20

# U Commands

- [udpTraffic on page 255](#)
- [udpv6Traffic on page 256](#)

### udpTraffic

---

<b>Description</b>	UDP frame transmit or receive
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Report all UDP receive or transmit events
<b>Filter 1</b>	<code>remote-ip-address <i>ipAddress</i> [ <i>ipAddressMask</i> ]</code> <ul style="list-style-type: none"><li>• remote-ip-address—Logs events for a remote address</li><li>• <i>ipAddress</i>—Address of remote system for which you want to log messages</li><li>• <i>ipAddressMask</i>—Mask for the remote address</li></ul>
<b>Filter 2</b>	<code>router <i>virtualRouterName</i> [ remote-ip-address <i>ipAddress</i> [ <i>ipAddressMask</i> ] ]</code> <ul style="list-style-type: none"><li>• router—Logs events on a specific virtual router</li><li>• <i>virtualRouterName</i>—Name of virtual router for which you want to log events</li><li>• remote-ip-address—Logs events for a remote address</li></ul>

- *ipAddress*—Address of remote system for which you want to log messages
- *ipAddressMask*—Mask for the remote address

## udpv6Traffic

---

<b>Description</b>	UDIPv6 packet transmit and receive events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	All UDIPv6 packet receive and transmit events
<b>Filter 1</b>	[ router <i>virtualRouterName</i> ] <ul style="list-style-type: none"><li>• router—Logs events for a specific virtual router</li><li>• <i>virtualRouterName</i>—Name of virtual router for which you want to log events</li></ul>
<b>Filter 2</b>	[ remote-ipv6-address <i>ipv6Address</i> ] <ul style="list-style-type: none"><li>• remote-ipv6-address—Logs events for packets arriving from or going to a specified IPv6 address</li><li>• <i>ipv6Address</i>—IPv6 address of remote system for which you want to log messages</li></ul>

## CHAPTER 21

# V Commands

- [vrrp on page 257](#)
- [vrrpTracking on page 258](#)
- [vsm on page 258](#)
- [vsmEngine on page 259](#)

### vrrp

---

<b>Description</b>	Virtual Router Redundancy Protocol
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	NVS error; out of resources; unexpected error
<b>Error</b>	Virtual router ID (VRID) creation or modification failure; association addresses creation or modification failure
<b>Warning Log</b>	IP interface used by VRRP was removed; unexpected advertisement received from neighbor; invalid authentication detected; unable to get IP interface's primary address
<b>Notice Log</b>	VRRP neighbor found
<b>Info</b>	State machine change
<b>Debug</b>	Management get, set, create, and remove
<b>Filter</b>	interface <i>interfaceType interfaceSpecifier</i> [ <i>vrrpIdentifier</i> ] <ul style="list-style-type: none"><li>• <i>interface</i>—Logs events on a specific interface</li><li>• <i>interfaceType</i>—Type of interface for which you want to log events</li><li>• <i>interfaceSpecifier</i>—Location of interface in the appropriate format</li></ul>



NOTE: For information about interface types and specifiers, see *Interface Types and Specifiers* in *JunosE Command Reference Guide*.

- *vrripIdentifier*—ID of the VRRP router for which you want to log events

---

## vrrpTracking

---

Description	Virtual Router Redundancy Protocol tracking
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Information about interaction between VRRP and the tracker module
Debug	Management get, set, create, and remove
Filter	None

---

## vsm

---

Description	VLAN subinterface manager
Emergency	None
Alert	None
Critical	Unable to find VLAN major interface for agent-circuit-id-based VLAN
Error	Truncating agent-circuit-id string
Warning Log	Creation failure
Notice Log	Out of pool space

<b>Info</b>	Replay of unknown interface after high availability switchover
<b>Debug</b>	General VSM operations, such as agent-circuit-id-based VLAN created
<b>Filter</b>	None

## vsmEngine

---

<b>Description</b>	VLAN subinterface manager engine
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Recoverable out-of-sync conditions after high availability switchover
<b>Filter</b>	None



## PART 3

# Index

- [Index on page 263](#)











**P**

platform considerations	
system logs.....	5

**S**

service commands	
service timestamps.....	14
show log commands	
show log configuration.....	16
show log data.....	16
support, technical	See technical support
system event logs	
individual logs.....	10, 13
severity.....	3
system-wide logs.....	10, 13
user-defined classification.....	15
verbosity.....	3
viewing logs.....	16

**T**

technical support	
contacting JTAC.....	xix
text and syntax conventions.....	xviii

