



**JUNOS[™]e Software
for E-series[™] Routing Platforms**

**System Event Logging
Reference Guide**

Release 9.0.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS 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 (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, and T320 routers, T640 routing node, and the JUNOS, JUNOSe, and SDX-300 software) 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.

Copyright © 2008, Juniper Networks, Inc.
All rights reserved. Printed in USA.

JUNOSe™ Software for E-series™ Routing Platforms System Event Logging Reference Guide, Release 9.0.x
Writing: Mark Barnard, Diane Florio, Bruce Gillham, Sarah Lesway-Ball, Brian Wesley Simmons, Fran Singer
Editing: Ben Mann
Cover Design: Edmonds Design

Revision History
29 February 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

	About This Guide	xiii
	Objectives	xiii
	Audience	xiii
	E-series Routers	xiv
	Documentation Conventions.....	xiv
	Related E-series and JUNOSe Documentation	xvi
	E-series and JUNOSe Documents	xvi
	JUNOSe Configuration Guides	xix
	Obtaining Documentation	xix
	Documentation Feedback	xx
	Requesting Technical Support	xx
	Self-Help Online Tools and Resources.....	xx
	Opening a Case with JTAC	xxi
Chapter 1	System Logging Overview	1
	Overview	1
	Log Severity	1
	Log Verbosity	2
	Persistent Logs	2
	Platform Considerations.....	2
	Configuring Event Logging	3
	Configuring Log Severity for Individual and Systemwide Logs	8
	Configuring Log Verbosity for Individual Logs or All Logs	12
	Setting the Timestamp for Log Messages	12
	Configuring Log Filters.....	14
	Turning Off Filters.....	15
	Monitoring Logging System Events	16
Chapter 2	Event Categories	21
	aaaAtm1483Cfg	21
	aaaEngineGeneral	22
	aaaQosCfg	22
	aaaServerGeneral	23
	aaaUserAccess	23
	addressServerGeneral	24
	ar1AaaServerGeneral	24
	atm	25
	atm1483	26
	atm1483VcClass	27
	atmAal5	27
	atmVcClass	28
	auditIpsec	28
	bfdAdaptivity	29

bfdEvents	29
bfdGeneral	30
bfdSession	30
bgpConnections	31
bgpDampening	32
bgpEvents	33
bgpGeneral	34
bgpGracefulRestart	35
bgpIpv6NextHops	36
bgpKeepAlives	37
bgpMessages	38
bgpNeighborChanges	39
bgpNextHops	40
bgpRoutes	41
bridge	44
bridgeEngine.....	44
bridgingMgr	45
bulkStats	45
cacGeneral	46
cacIntf	46
cliCommand	47
cliGeneral	47
connectionManager	48
cops	48
copsPr	49
coreDump	49
ctreeLog	50
dcm	50
dcmEngineGeneral	51
dhcpCapture	51
dhcpExternal	52
dhcpExternalEngine	52
dhcpGeneral	53
dhcpIssuLog.....	53
dhcpLocalClients	54
dhcpLocalGeneral.....	55
dhcpLocalHighAvailability	55
dhcpLocalPool.....	56
dhcpLocalProtocol	57
dhcpNvGeneral	58
dhcpOfferLog	58
dhcpPbeGeneral	59
dhcpProxyGeneral	59
dhcpRelayGeneral	60
dhcpv6Client	60
dhcpv6DemuxGeneral	61
dhcpv6LsGeneral	61
dismanEventManager	62
dnsGeneralLog	62
dosProtection.....	63
ds1	63
ds3	64
dvmrpGeneral	64
dvmrpGracefulRestart	65

dvmrpMcastTable	66
dvmrpProbeRcv	67
dvmrpProbeSent	67
dvmrpRtTable	68
ethernet	68
ethernetStateSession	69
fileSystem	69
flowInspection	70
flowInspectionEngine	70
flowServicesFirewallAlert	71
flowServicesFirewallAudit	71
frameRelay	72
fsAgent	72
ft1	73
ftpClient	73
ftpServer	74
gplaan	74
ha	75
hdlc	75
hotfixGeneral	76
httpServer	77
icImageFixServer	78
icmpTraffic	79
icmpv6Traffic	80
igmpGeneral	81
igmpGracefulRestart	82
igmpGroupState	83
ikeCertificateMgr	84
ikeEnrollment	84
ikepki	85
interModuleCommunication	85
ipAccessList	86
ipEngine	87
ipflowstats	87
ipflowstatsEngine	88
ipGeneral	88
ipIfCreator	89
ipInterface	90
ipNhopTrackerGeneral	90
ipProfileMgr	91
ipRoutePolicy	91
ipRouteTable	92
ipsecIdDb	92
ipsecP1Throttler	93
ipsecXcfgSM	93
ipSubscriberMgr	94
ipTraffic	94
ipTunnel	95
ipv6AccessList	96
ipv6General	97
ipv6Interface	98
ipv6ProfileMgr	98
ipv6RouteTable	99
ipv6Traffic	100

ipv6Types	101
isisAdjChange	102
isisAdjPackets	103
isisBfdEvents	103
isisChecksumErr	104
isisGeneral	104
isisHelloGeneral	105
isisHelloPackets	105
isisIpv6Log	106
isisLdpEvents	106
isisLocalUpdate	107
isisMplsTeAdvertisements	107
isisMplsTeEvents	108
isisNsfEvents	108
isisProtocolErr	109
isisSnppackets	109
isisSpfEvents	110
isisSpfStatistics	110
isisSpfTriggers	111
isisUpdatePackets	111
isVoice	112
itm	112
l2cGeneral	113
l2cKeepAlive	113
l2cPacket	114
l2tp	114
l2tpDialoutGenerator	115
l2tpDisconnectCause	115
l2tpIpLowerBinding	116
l2tpStateMachine	116
ldpConnect	117
ldpGeneral	117
ldpGracefulRestart	118
ldpHelloMessages	118
ldpHelloMgr	119
ldpInterface	120
ldpMessages	121
ldpPeer	121
ldpShimInterface	122
ldpSocket	123
ldpTimer	123
ldpVpls	124
ldpWorker	124
localAddressServerGeneral	125
localAuthServer	125
localEnableAuthServer	126
localLinePassword	126
macroData	127
mgmtGeneral	127
mgmtGracefulRestart	128
mgmtmv6General	129
mgmtmv6GracefulRestart	130
mldGeneral	131
mldGracefulRestart	132

mldGroupState	133
mmcd	134
mobileIpv4HaBinding	134
mobileIpv4HaEng	135
mobileIpv4HaEvent	135
mobileIpv4HaLog	136
mplsFwdTable.....	136
mplsGeneral.....	137
mplsHighAvailability	137
mplsMajorInterface	138
mplsMinorInterface.....	139
mplsRouter	140
mplsShimInterface	141
mplsTraffic.....	142
mrInfoLog	142
mrInfoRcvdLog	143
mrInfoSentLog	143
mtraceLog	144
mtraceRcvdLog	144
mtraceSentLog	145
multicastTraffic	146
nameResolverLog	147
nfsClient.....	147
noneAaaAddrServer	148
noneAaaServer	148
ntpGeneral	149
os	150
ospfElectDr	151
ospfGeneral	152
ospfHelloPktsRcvd	153
ospfHelloPktsSent	154
ospfInterface	155
ospfLdpEvents	155
ospfLsa	156
ospfNeighbor	157
ospfPktsRcvd	157
ospfPktsSent	158
ospfRestart	158
ospfRoute	159
ospfSpfExt	159
ospfSpfInter	160
ospfSpfIntra	160
ospfTeDatabase	161
ospfTeSpf.....	161
ospfv3ElectDr	162
ospfv3General	163
ospfv3HelloPktsRcvd.....	164
ospfv3HelloPktsSent	165
ospfv3Interface	166
ospfv3Lsa	167
ospfv3Neighbor	168
ospfv3PktsRcvd	169
ospfv3PktsSent	169
ospfv3Route	170

ospfV3SpfExt	170
ospfV3SpfInter	171
ospfV3SpfIntra	171
pimAutoRPRcvdLog	172
pimAutoRPSentLog	173
pimBsrRcvdLog	174
pimBsrSentLog	174
pimGracefulRestartLog	175
pimHelloRcvdLog	175
pimHelloSentLog	176
pimIpv6AutoRPRcvdLog	176
pimIpv6AutoRPSentLog	178
pimIpv6BsrRcvdLog	178
pimIpv6BsrSentLog	179
pimIpv6GracefulRestartLog	179
pimIpv6HelloRcvdLog	180
pimIpv6HelloSentLog	181
pimIpv6PktsRcvdLog	182
pimIpv6PktsSentLog	182
pimPktsRcvdLog	183
pimPktsSentLog	183
pimsmGeneral	184
pimsmMvpn	184
policyMgrAttachment	185
policyMgrGeneral	185
policyMgrPacketLog	186
ppp	186
pppoe	187
pppoeControlPacket	188
pppPacket	189
pppStateMachine	190
profileMgr	191
qm	191
qos	192
qosAttachment	192
radiusAttributes	193
radiusClient	193
radiusCoAAttributes	194
radiusDisconnectGeneral	194
radiusRelayGeneral	195
radiusSendAttributes	195
remOps	196
resourceThresholdTrap	196
ripBfd	197
ripGeneral	198
ripRoute	199
ripRtTable	200
routeDownloader	200
routerLog	201
rsvpAsyncMgr	201
rsvpBfd	202
rsvpGeneral	202
rsvpGracefulRestart	203
rsvpInterface	204

rsvpTunnel	205
security	205
serviceability	206
serviceMgr	206
serviceMgrClientSession	207
serviceMgrDcm	207
serviceMgrMacroManager	208
serviceMgrPerformance	208
serviceMgrServiceDef	209
serviceMgrServiceInstance	209
serviceMgrServiceSession	210
serviceMgrSubscriberSession	210
slep	211
snmp	211
snmpIfMib	212
snmpPduAudit	212
snmpSetPduAudit	213
snmpTrap	213
sonet	214
sonetPath	214
sonetVT	215
ssccDetailPm	215
ssccDetailSsc	216
ssccGeneral	216
ssh	217
stTunnel	217
stTunnelEngine	218
system	219
tacacsPlusServer	220
tcpGeneral	220
tcpTraffic	221
tcpv6Traffic	222
telnet	223
telnetClient	223
tftpClient	224
trackerEvents	224
trackerGeneral	225
tsm	225
udpTraffic	226
udpv6Traffic	227
vrrp	228
vrrpTracking	229
vsm	229
vsmEngine	230

Index**231**

About This Guide

This preface provides the following guidelines for using the *JUNOS[™] Software for E-series[™] Routing Platforms System Event Logging Reference Guide*:

- Objectives on page xiii
- Audience on page xiii
- E-series Routers on page xiv
- Documentation Conventions on page xiv
- Related E-series and JUNOS[™] Documentation on page xvi
- Obtaining Documentation on page xix
- Documentation Feedback on page xx
- Requesting Technical Support on page xx

Objectives

This guide describes the JUNOS[™] software's system logging feature and describes how to use the CLI to monitor your system's log configuration and system events.

An E-series router is shipped with the latest system software installed. If you need to install a future release or reinstall the system software, refer to the procedures in *JUNOS[™] System Basics Configuration Guide, Chapter 3, Installing JUNOS[™] Software*.



NOTE: If the information in the latest *JUNOS[™] Release Notes* differs from the information in this guide, follow the *JUNOS[™] Release Notes*.

Audience

This guide is intended for experienced system and network specialists working with E-series routers in an Internet access environment.

E-series Routers

Seven models of E-series routers are available:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

All models use the same software. For information about all models except the E120 router and the E320 router, see *ERX Hardware Guide, Chapter 1, ERX Overview*. For information about the E120 router and the E320 router, see *E120 and E320 Hardware Guide, Chapter 1, E120 and E320 Overview*.

In the E-series documentation, the term ERX-14xx models refers to both the ERX-1440 router and the ERX-1410 router. Similarly, the term ERX-7xx models refers to both the ERX-710 router and the ERX-705 router. The terms ERX-1440 router, ERX-1410 router, ERX-710 router, ERX-705 router, ERX-310 router, E120 router, and E320 router refer to the specific models.

Documentation Conventions

Table 1 defines notice icons used in this guide.

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.

Table 2 defines text conventions used in this guide and the syntax conventions used primarily in the *JUNOS Command Reference Guide*. For more information about command syntax, see *JUNOS System Basics Configuration Guide, Chapter 2, Command-Line Interface*.

Table 2: Text and Syntax Conventions

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

Related E-series and JUNOS Documentation

The E-series and JUNOS documentation set consists of several hardware and software guides, which are available in electronic and printed formats.

E-series and JUNOS Documents

Table 3 lists and describes the E-series and JUNOS document set. For a complete list of abbreviations used in this document set, along with their spelled-out terms, see *JUNOS System Basics Configuration Guide, Appendix A, Abbreviations and Acronyms*.

Table 3: Juniper Networks E-series and JUNOS Technical Publications

Document	Description
E-series Hardware Documentation	
<i>E120 and E320 Quick Start Guide</i>	Shipped in the box with all new E120 and E320 routers. Provides the basic procedures to help you get the routers up and running quickly.
<i>E120 and E320 Hardware Guide</i>	<p>Provides the necessary procedures for getting E120 routers and E320 routers operational, including information about:</p> <ul style="list-style-type: none"> ■ Installing the chassis and modules ■ Connecting cables ■ Powering up the routers ■ Configuring the routers for management access ■ Troubleshooting common issues <p>Describes switch route processor (SRP) modules, line modules, and I/O adapters (IOAs) available for E120 and E320 routers.</p>
<i>E120 and E320 Module Guide</i>	<p>Provides detailed specifications for line modules and IOAs in E120 and E320 routers, and information about the compatibility of these modules with JUNOS software releases.</p> <p>Lists the layer 2 protocols, layer 3 protocols, and applications that line modules and their corresponding IOAs support.</p> <p>Provides module LED information.</p>
<i>E-series Installation Quick Start poster or ERX Quick Start Guide</i>	Shipped in the box with all new ERX routers. Provides the basic procedures to help you get an ERX router up and running quickly.
<i>ERX Hardware Guide</i>	<p>Provides the necessary procedures for getting ERX-14xx models, ERX-7xx models, and ERX-310 routers operational, including information about:</p> <ul style="list-style-type: none"> ■ Installing the chassis and modules ■ Connecting cables ■ Powering up the routers ■ Configuring the routers for management access ■ Troubleshooting common issues <p>Describes switch route processor (SRP) modules, line modules, and I/O modules available for the ERX routers.</p>
<i>ERX Module Guide</i>	<p>Provides detailed specifications for line modules and I/O modules in ERX-14xx models, ERX-7xx models, and ERX-310 routers, and information about the compatibility of these modules with JUNOS software releases.</p> <p>Lists the layer 2 protocols, layer 3 protocols, and applications that line modules and their corresponding I/O modules support.</p> <p>Provides module LED information.</p>

Table 3: Juniper Networks E-series and JUNOS® Technical Publications (continued)

Document	Description
<i>ERX End-of-Life Module Guide</i>	Provides an overview and description of ERX modules that are end-of-life (EOL) and can no longer be ordered for the following routers: <ul style="list-style-type: none"> ■ ERX-7xx models ■ ERX-14xx models ■ ERX-310 router
JUNOS® Software Guides	
<i>JUNOS® System Basics Configuration Guide</i>	Provides information about: <ul style="list-style-type: none"> ■ Planning and configuring your network ■ Using the command-line interface (CLI) ■ Installing JUNOS® software ■ Configuring the Simple Network Management Protocol (SNMP) ■ Managing the router and its modules, including the use of high availability (HA) for SRP redundancy ■ Configuring and running a unified in-service software upgrade (ISSU) ■ Configuring passwords and security ■ Configuring the router clock ■ Configuring virtual routers
<i>JUNOS® Physical Layer Configuration Guide</i>	Explains how to configure, test, and monitor physical layer interfaces.
<i>JUNOS® Link Layer Configuration Guide</i>	Explains how to configure and monitor static and dynamic link layer interfaces.
<i>JUNOS® IP, IPv6, and IGP Configuration Guide</i>	Explains how to configure and monitor IP, IPv6 and Neighbor Discovery, and interior gateway protocols (RIP, OSPF, and IS-IS).
<i>JUNOS® IP Services Configuration Guide</i>	Explains how to configure and monitor IP routing services. Topics include: <ul style="list-style-type: none"> ■ Routing policies ■ Firewalls ■ Network Address Translation (NAT) ■ J-Flow statistics ■ Bidirectional forwarding detection (BFD) ■ Internet Protocol Security (IPSec) ■ Access Node Control Protocol (ANCP), also known as Layer 2 Control (L2C) ■ Digital certificates ■ IP tunnels ■ Virtual Router Redundancy Protocol (VRRP) ■ Mobile IP home agent
<i>JUNOS® Multicast Routing Configuration Guide</i>	Explains how to configure and monitor IP multicast routing and IPv6 multicast routing. Topics include: <ul style="list-style-type: none"> ■ Internet Group Management Protocol (IGMP) ■ Protocol Independent Multicast (PIM) ■ Distance Vector Multicast Routing Protocol (DVMRP) ■ Multicast Listener Discovery (MLD)

Table 3: Juniper Networks E-series and JUNOS Technical Publications (continued)

Document	Description
<i>JUNOS BGP and MPLS Configuration Guide</i>	Explains how to configure and monitor: <ul style="list-style-type: none"> ■ Border Gateway Protocol (BGP) routing ■ Multiprotocol Label Switching (MPLS) and related applications ■ Layer 2 services over MPLS ■ Virtual private LAN service (VPLS) ■ Layer 2 virtual private networks (L2VPNs)
<i>JUNOS Policy Management Configuration Guide</i>	Explains how to configure, manage, and monitor customized policy rules for packet classification, forwarding, filtering, and flow rates. Also describes the packet mirroring feature, which uses secure policies.
<i>JUNOS Quality of Service Configuration Guide</i>	Explains how to configure quality of service (QoS) features to queue, schedule, and monitor traffic flow. These features include: <ul style="list-style-type: none"> ■ Traffic classes and traffic-class groups ■ Drop, queue, QoS, and scheduler profiles ■ QoS parameters ■ Statistics
<i>JUNOS Broadband Access Configuration Guide</i>	Explains how to configure and monitor a remote access environment, which can include the following features: <ul style="list-style-type: none"> ■ Authentication, authorization, and accounting (AAA) ■ Dynamic Host Configuration Protocol (DHCP) ■ Remote Authentication Dial-In User Service (RADIUS) ■ Terminal Access Controller Access Control System (TACACS+) ■ Layer 2 Tunneling Protocol (L2TP) ■ Subscriber management
<i>JUNOS System Event Logging Reference Guide</i>	Describes the JUNOS system logging feature and describes how to use the CLI to monitor your system's log configuration and system events.
<i>JUNOS Command Reference Guide A to M:</i> <i>JUNOS Command Reference Guide N to Z</i>	Together constitute the <i>JUNOS Command Reference Guide</i> . Contain important information about commands implemented in the system software. Use to look up: <ul style="list-style-type: none"> ■ Descriptions of commands and command parameters ■ Command syntax ■ A command's related mode ■ Starting with JUNOS Release 7.1.0, a history of when a command, its keywords, and its variables were introduced or added Use with the JUNOS configuration guides.
<i>JUNOS Comprehensive Index</i>	Provides a complete index of the JUNOS software documentation set.
<i>JUNOS Glossary</i>	Provides definitions for terms used in JUNOS technical documentation.
Release Notes	
<i>JUNOS Release Notes</i>	Provide the latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the <i>Release Notes</i> differs from the information found in the documentation set, follow the <i>Release Notes</i> . Release notes are included on the corresponding software CD and are available on the Web.

JUNOS^e Configuration Guides

JUNOS^e software configuration guides use a bottom-up approach to describe the relationship of layers, protocols, and interfaces in the configuration process. For more information, see *Layered Approach* in *JUNOS^e System Basics Configuration Guide, Chapter 1, Planning Your Network*.

The chapters in JUNOS^e software configuration guides typically include the following topics:

- Conceptual and overview information
- Information you need to know or tasks you need to perform before you begin
- Platform-specific issues you need to take into consideration
- Applicable references, such as RFCs and IETF draft documents, about the protocols and features supported by the router
- Required and optional tasks, as step-by-step procedures
- Descriptions and examples of the commands you use
- Illustrations of network topologies
- Examples of command sequences for configuration, testing, and monitoring activities
- Sample displays that result when you issue the **show** command

Obtaining Documentation

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

To order printed copies of this manual and other Juniper Networks technical documents or to order a documentation CD, which contains this manual, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the software CDs and 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, or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- 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, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- **JTAC Policies**—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/customers/support/downloads/710059.pdf>
- **Product Warranties**—For product warranty information, visit <http://www.juniper.net/support/warranty/>
- **JTAC Hours of Operation**—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings:
<http://www.juniper.net/customers/support/>
- Search for known bugs:
<http://www2.juniper.net/kb/>
- Find product documentation:
<http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base:
<http://kb.juniper.net/>
- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications:
<https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager:
<http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at
<https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Manager tool in the CSC at
<http://www.juniper.net/cm/>
- Call 1-888-314-JTAC (1-888-314-5822 – toll free in the USA, Canada, and Mexico)

For international or direct-dial options in countries without toll-free numbers, visit
<http://www.juniper.net/support/requesting-support.html>

Chapter 1

System Logging Overview

E-series 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 on page 1
- Platform Considerations on page 2
- Configuring Event Logging on page 3
- Monitoring Logging System Events on page 16

Overview

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 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 *Chapter 2, Event Categories*.

Table 4: 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.

Log messages are not synchronized between primary and redundant SRP modules. During a switchover from a primary to a redundant SRP module, existing log messages are not transferred to the redundant SRP module.

Platform Considerations

System logs are supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Configuring Event Logging

By default, event logging is enabled and has default settings. This section explains how to change settings to customize event logging to fit your needs.

- Set a baseline for when the system begins logging messages.

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

- Set the log severity.

```
host1(config)#log severity warning
```

- Remove the limit on the number of buffers available for an event category.

```
host1(config)#log unlimit qos
```

- Set the log verbosity.

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

- Log messages to a specified destination.

```
host1(config)#log destination syslog 10.10.9.5 include ospfGeneral
mplsGeneral os
```

- Select fields to be added to logs.

```
host1(config)#log fields timestamp instance no-calling-task
```

- Enable logs destined for a console to be displayed at the current console device.

```
host1#log here
```

The next sections explain how to configure individual and systemwide logs, how to format timestamps for log messages, and how to configure log filters.

baseline log

- Use to set a baseline for logging events. Only log messages timestamped after the baseline appear when you enter the **show log data delta** command.
- To use the current system time, do not enter any options.
- To set a specific time, use the following syntax:

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.

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 enter a command excluding certain categories and then follow it with a command including others.
 - You can issue successive **include** commands or successive **exclude** commands; in this case, the successive commands expand the list of included or excluded categories.

- Example 1—The first command causes *only* the ospfGeneral, mplsGeneral, and os event categories to be logged to system log at 10.10.9.5. The second command reverses this inclusion and restores the logging of *all* event categories.

```
host1(config)#log destination syslog 10.10.9.5 include ospfGeneral
mplsGeneral os
host1(config)#no log destination syslog 10.10.9.5
```

- Example 2—The first command again causes only the ospfGeneral, mplsGeneral, and os event categories to be logged to system log at 10.10.9.5. The second command reverses the inclusion of ospfGeneral and os. The mplsGeneral category is still included and is thus the *only* category logged.

```
host1(config)#log destination syslog 10.10.9.5 include ospfGeneral mplsGeneral
os
host1(config)#no log destination syslog 10.10.9.5 include ospfGeneral os
```

- Example 3—The first command causes the isisGeneral, ipRoutePolicy, and ipTraffic event categories to be excluded from logging to system log at 10.1.2.3. The second command reverses this exclusion and restores the logging of *all* event categories.

```
host1(config)#log destination syslog 10.1.2.3 exclude isisGeneral ipRoutePolicy
ipTraffic
host1(config)#no log destination syslog 10.1.2.3 exclude
```

- Example 4—The first command again causes the isisGeneral, ipRoutePolicy, and ipTraffic event categories to be excluded from logging to system log at 10.1.2.3. The second command reverses the exclusion of ipRoutePolicy and ipTraffic. The isisGeneral category is still excluded; all other events are logged.

```
host1(config)#log destination syslog 10.1.2.3 exclude isisGeneral
ipRoutePolicy ipTraffic
host1(config)#no log destination syslog 10.1.2.3 exclude isisGeneral
```

- Example 5—The first command causes the isisGeneral event category to be excluded from logging to system log at 10.1.2.3. The second command causes ospfGeneral to also be excluded from logging.

```
host1(config)#log destination syslog 10.1.2.3 exclude isisGeneral
host1(config)#log destination syslog 10.1.2.3 exclude ospfGeneral
```

- Example 6—The first command causes the isisGeneral event category to be excluded from logging to system log at 10.1.2.3; all other events are logged. The second command overrides the first and causes the exclusion of all events except ospfGeneral.

```
host1(config)#log destination syslog 10.1.2.3 exclude isisGeneral
host1(config)#log destination syslog 10.1.2.3 include ospfGeneral
```

- Use the **no** version to reverse the effects of previous commands or restore the default, which is to log all event categories.

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.

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.

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.

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.

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 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 8 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 *
```

log unlimit

- 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 unlimit qos
```

- Use the **no** version to return to the default value.

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.

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
```

category	severity	verbosity	filters	notes
-----	-----	-----	-----	-----
aaaAtm1483Cfg	ERROR	low		
aaaEngineGeneral	ERROR	low		
aaaServerGeneral	ERROR	low		
aaaUserAccess	ERROR	low		
addressServerGeneral	ERROR	low		
ar1AaaServerGeneral	ERROR	low		
atm	ERROR	low		
atm1483	ERROR	low		
atmAa15	ERROR	low		

Notice that the atm event category has a default severity of Error.

2. Change all event categories to Warning, systemwide, and view the log configuration:

```
host1(config)#log severity warning
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
log severity WARNING
```

category	severity	verbosity	filters	notes
-----	-----	-----	-----	-----
aaaAtm1483Cfg	WARNING	low		1
aaaEngineGeneral	WARNING	low		1
aaaServerGeneral	WARNING	low		1
aaaUserAccess	WARNING	low		1
addressServerGeneral	WARNING	low		1
ar1AaaServerGeneral	WARNING	low		1
atm	WARNING	low		1
atm1483	WARNING	low		1
atmAa15	WARNING	low		1

3. Change the atm category to have a log severity of Emergency and view the log configuration:

```

host1(config)#log severity emergency atm
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
log severity WARNING

category	severity	verbosity	filters	notes
-----	-----	-----	-----	-----
aaaAtm1483Cfg	WARNING	low		1
aaaEngineGeneral	WARNING	low		1
aaaServerGeneral	WARNING	low		1
aaaUserAccess	WARNING	low		1
addressServerGeneral	WARNING	low		1
ar1AaaServerGeneral	WARNING	low		1
atm	EMERGENCY	low		2
atm1483	WARNING	low		1
atmAa15	WARNING	low		1

4. Change all event categories to Alert, systemwide, and view the log configuration:

```

host1(config)#log severity alert
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
log severity ALERT

category	severity	verbosity	filters	notes
-----	-----	-----	-----	-----
aaaAtm1483Cfg	ALERT	low		1
aaaEngineGeneral	ALERT	low		1
aaaServerGeneral	ALERT	low		1
aaaUserAccess	ALERT	low		1
addressServerGeneral	ALERT	low		1
ar1AaaServerGeneral	ALERT	low		1
atm	EMERGENCY	low		2
atm1483	ALERT	low		1
atmAa15	ALERT	low		1

Notice that the atm event category that you individually assigned in Step 3 does not change.

- Turn off log notification, systemwide, and view the log configuration:

```
host1(config)#log severity off
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
log severity OFF
```

category	severity	verbosity	filters	notes
-----	-----	-----	-----	-----
aaaAtm1483Cfg	OFF	low		1
aaaEngineGeneral	OFF	low		1
aaaServerGeneral	OFF	low		1
aaaUserAccess	OFF	low		1
addressServerGeneral	OFF	low		1
ar1AaaServerGeneral	OFF	low		1
atm	EMERGENCY	low		2
atm1483	OFF	low		1
atmAa15	OFF	low		1

Notice that the atm event category does not change.

- Remove the assigned status of the atm event category and view the log configuration:

```
host1(config)#no log severity atm
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
log severity OFF
```

category	severity	verbosity	filters	notes
-----	-----	-----	-----	-----
aaaAtm1483Cfg	OFF	low		1
aaaEngineGeneral	OFF	low		1
aaaServerGeneral	OFF	low		1
aaaUserAccess	OFF	low		1
addressServerGeneral	OFF	low		1
ar1AaaServerGeneral	OFF	low		1
atm	OFF	low		1
atm1483	OFF	low		1
atmAa15	OFF	low		1

Notice that the atm event category follows the systemwide severity level of OFF. The systemwide setting takes precedence over the atm event category default of Error.

- Change all event categories, systemwide, to their default/unassigned levels, and view the log configuration:

```

host1(config)#no log severity *
Please wait...
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

```

category	severity	verbosity	filters	notes
-----	-----	-----	-----	-----
aaaAtm1483Cfg	ERROR	low		
aaaEngineGeneral	ERROR	low		
aaaServerGeneral	ERROR	low		
aaaUserAccess	ERROR	low		
addressServerGeneral	ERROR	low		
ar1AaaServerGeneral	ERROR	low		
atm	ERROR	low		
atm1483	ERROR	low		
atmAa15	ERROR	low		

Configuring Log Verbosity for Individual Logs or All Logs

The default verbosity setting for all logs is low. To change the logging verbosity of an individual log, specify a category when you enter the **log verbosity** command. To change the log verbosity of every log, do not specify an event category when you enter the **log verbosity** command. However, after you enter the **log verbosity** command without specifying a particular event category, all logs are set to the new verbosity. No log verbosity overrides are saved.

Example The following example sets all log categories to verbosity medium, and then it sets the verbosity level for ds3 events to high.

```

host1(config)#log verbosity medium
host1(config)#log verbosity high ds3

```

Setting the Timestamp for Log Messages

You can use the **service timestamps** command to format timestamps for log messages. By default, log messages display universal coordinated time (UTC) without the time zone.

The following examples illustrate how you can change the timestamp on log messages.

- Set the time zone to eastern daylight time (EDT), 5 hours behind UTC, and display the local time on the log messages.

```

host1(config)#clock timezone EDT -5

```

- Display UTC, but no time zone, on the log messages.

```
host1(config)#service timestamps log datetime
host1#exit
host1#show log data category cliCommand severity info
*****
NOTICE 05/14/2001 18:24:49 cliCommand: "configure terminal", console
NOTICE 05/14/2001 18:24:45 cliCommand: "service timestamps log datetime",
console
*****
```

- Display UTC and the time zone on the log messages.

```
host1#configure terminal
host1(config)#service timestamps log datetime show-timezone
host1(config)#exit
host1#show log data category cliCommand severity info
*****
NOTICE 05/14/2001 18:28:45 UTC EDT cliCommand: "configure terminal", console
NOTICE 05/14/2001 18:28:42 UTC EDT cliCommand: "service timestamps log
datetime show-timezone", console
*****
```

- Display no timestamp on the log messages.

```
host1#configure terminal
host1(config)#no service timestamps
host1#exit
host1#show log data category cliCommand severity info
*****
NOTICE 134 cliCommand: "configure terminal", console
NOTICE 133 cliCommand: "no service timestamps", console
*****
```

service timestamps

- Use to format timestamps for log messages.
- For information about setting local times and time zones, see *JUNOS System Basics Configuration Guide, Chapter 12, Configuring the System Clock*.
- The **show log data** command displays the log data with the current timestamp format.
- The **show log data nv-file** command displays the log data with the timestamp format in effect at the time the log record was written.
- Use the **no** version to remove timestamps from log messages.

Configuring Log Filters

Many event categories contain filters so you can further refine the type of information that the system logs. For example, when logging BGP connections, you can limit the information logged to a specific access class, peer, route map, or virtual router.

You define filters when you set the log severity for an event category. The online Help shows the options you can set for each filter.



NOTE: You can use the packet flow monitoring feature to create user-defined classification parameters that specify the packet data that is logged. See *Packet Tagging Overview* in *JUNOS Policy Management Configuration Guide, Chapter 4, Creating Classifier Groups and Policy Rules*.

The following example creates a filter that logs BGP connection information at the debug severity level on traffic that matches access list ListOne, and is incoming traffic to virtual router default.

```
host1(config)#log severity debug bgpevents ?
  access-class  Select an access list for the filter
  in            Select import/in direction for the filter
  out          Select export/out direction for the filter
  peer         Select a peer IP address for the filter
  route-map    Select a route map for the filter
  router       Identify an instance of a virtual router
  <cr>

host1(config)#log severity debug bgpevents access-class ?
  WORD  The access list

host1(config)#log severity debug bgpevents access-class ListOne ?
  filtering-router Identify virtual router where access-class/route-map are defined
  in              Select import/in direction for the filter
  out            Select export/out direction for the filter
  route-map      Select a route map for the filter
  <cr>

host1(config)#log severity debug bgpevents access-class ListOne route-map ?
  WORD  The route map

host1(config)#log severity debug bgpevents access-class ListOne route-map default ?
  filtering-router Identify virtual router where access-class/route-map are defined
  in              Select import/in direction for the filter
  out            Select export/out direction for the filter
  <cr>

host1(config)#log severity debug bgpevents access-class ListOne route-map default in
```

The next example limits the logging of PPP debug events to traffic to or from the POS interface in slot 2/0.

```
host1(config)#log severity debug ppp ?
  atm          Specify an ATM PPP interface
  fastEthernet Specify a fastEthernet interface
  gigabitEthernet Specify a gigabitEthernet interface
  mlppp        Specify an MLPPP network interface
  pos          Specify a POS PPP interface
  serial       Specify a serial PPP interface
  <cr>
host1(config)#log severity debug ppp pos 2/0
```

To obtain a list of the filters available in each event category, see *Chapter 2, Event Categories*.

Turning Off Filters

You can turn off filters in three ways:

- Turn off all filters
- Turn off all filters for an event category
- Turn off a specific filter

To turn off all filters:

```
host1(config)#no log filters
```

To turn off all filters for an event category, use the **no** version of the **log severity** command along with the category name. For example:

```
host1(config)#no log severity bgpEvents filters
```

To turn off a specific filter, use the **no** version of the **log severity** command that you used to add the filter. For example:

```
host1(config)#no log severity bgpEvents peer 10.0.0.2 10.0.0.1
```

no log filters

- Use to turn off log filters.
- To turn off all filters for an event category, specify the category name.
- Example

```
host1(config)#no log filters
```

- To turn off a specific filter, use the **no** version of the **log severity** command that you used to add the filter.

Monitoring Logging System Events

Use the **show log configuration** command to display your log configuration. Use the **show log data** command to display system events on your screen.

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *show Commands* in *JUNOS System Basics Configuration Guide, Chapter 2, Command-Line Interface* for details.

show log configuration

- Use to show the logging configuration on your system.
- Example 1—Factory defaults are set

```
host1#show log configuration
log destination console severity WARNING
log destination nv-file severity CRITICAL
no log engineering
log fields timestamp instance no-calling-task
no log severity
```

category	severity	verbosity	filters
-----	-----	-----	-----
NameResolverLog	ERROR	low	
aaaAtm1483Cfg	ERROR	low	
aaaEngineGeneral	ERROR	low	
aaaServerGeneral	ERROR	low	
addressServerGeneral	ERROR	low	
atm	ERROR	low	
atm1483	ERROR	low	
atmAal5	ERROR	low	
bgpConnections	ERROR	low	
...			
cliCommand	NOTICE	low	
controlNetworkSlave	ERROR	low	
cops	ERROR	low	
...			
udpTraffic	ERROR	low	

- Example 2—Individual log **udpTraffic** is set to warning

```
host1#(config)#log severity warning udpTraffic
host1##show log configuration
log destination console severity WARNING
log destination nv-file severity CRITICAL
no log engineering
log fields timestamp instance no-calling-task
no log severity
```

category	severity	verbosity	filters
-----	-----	-----	-----
NameResolverLog	ERROR	low	
aaaAtm1483Cfg	ERROR	low	
aaaEngineGeneral	ERROR	low	
aaaServerGeneral	ERROR	low	
addressServerGeneral	ERROR	low	
atm	ERROR	low	
atm1483	ERROR	low	
atmAa15	ERROR	low	
bgpConnections	ERROR	low	
...			
cliCommand	NOTICE	low	
controlNetworkSlave	ERROR	low	
cops	ERROR	low	
...			
udpTraffic	WARNING*	low	

* Default severity setting is overridden by the individual log severity setting.

- Example 3—**Log severity** is set to alert

```
host1#(config)#log severity alert
host1##show log configuration
log destination console severity WARNING
log destination nv-file severity CRITICAL
no log engineering
log fields timestamp instance no-calling-task
log severity ALERT
```

category	severity	verbosity	filters
-----	-----	-----	-----
NameResolverLog	ALERT#	low	
aaaAtm1483Cfg	ALERT#	low	
aaaEngineGeneral	ALERT#	low	
aaaServerGeneral	ALERT#	low	
addressServerGeneral	ALERT#	low	
atm	ALERT#	low	
atm1483	ALERT#	low	
atmAa15	ALERT#	low	
bgpConnections	ALERT#	low	
...			
cliCommand	ALERT#	low	
controlNetworkSlave	ALERT#	low	
cops	ALERT#	low	
...			
udpTraffic	ALERT#	low	

* Default severity setting is overridden by the system-wide severity setting.

- Example 4—Individual log **atm** is set to severity warning

```

host1#(config)#log severity warning atm
host1#show log configuration
  log destination console severity WARNING
  log destination nv-file severity CRITICAL
  no log engineering
  log fields timestamp instance no-calling-task
  log severity ALERT

```

category	severity	verbosity	filters
-----	-----	-----	-----
NameResolverLog	ALERT#	low	
aaaAtm1483Cfg	ALERT#	low	
aaaEngineGeneral	ALERT#	low	
aaaServerGeneral	ALERT#	low	
addressServerGeneral	ALERT#	low	
atm	WARNING*	low	
atm1483	ALERT#	low	
atmAa15	ALERT#	low	
bgpConnections	ALERT#	low	
...			
cliCommand	ALERT#	low	
controlNetworkSlave	ALERT#	low	
cops	ALERT#	low	
...			
udpTraffic	ALERT#	low	

* Default severity setting is overridden by the system-wide severity setting.

* Default severity setting is overridden by the individual log severity setting.

show log data

- Use to display system events.
- Use keywords to select which events are displayed:
 - **category**—Limits the display to a single log event category. See the CLI online Help for available categories.

- Example

```
host1#show log data category os
```

- **delta**—Limits the display to events that occurred after the time set with the log baseline command.
- **nv-file**—Displays the information that is currently logged to nonvolatile storage.

- Example

```
host1#show log data nv-file
logFile.temp: The system cannot find the file specified.
ALERT 09/12/2000 21:29:17 os: ASSERTION FAILED: file mplsNvs2.cc, line 789
ALERT 09/20/2000 02:18:06 os: ASSERTION FAILED: file osPool.cc, line 819
ALERT 09/20/2000 02:26:35 os: ASSERTION FAILED: file osPool.cc, line 819
ALERT 09/20/2000 02:44:33 os: ASSERTION FAILED: file osPool.cc, line 819
ALERT 09/20/2000 04:56:35 os: ASSERTION FAILED: file osPool.cc, line 819
ALERT 09/27/2000 03:10:25 os: ASSERTION FAILED: file
/sw0/sc/nvs/include/./nvMapBackend.h, line 235
ALERT 10/02/2000 04:05:42 os: ASSERTION FAILED: file osHeap.cc, line 439
ALERT 10/02/2000 04:08:04 os: ASSERTION FAILED: file osMessageQueue.cc, line
42, rip1
ALERT 10/12/2000 03:43:38 os: PANIC: file osSemaphore.cc, line 54
ALERT 11/01/2000 02:03:49 os: ASSERTION FAILED: file cliCommand.cc, line 195
```

- **severity**—Displays events that have a specific severity level.

- Example

```
host1#show log data severity notice
NOTICE 01/10/2001 00:59:50 os: config -- using running
NOTICE 01/10/2001 00:59:52 os: srp application, build date: 0x3a437424 (FRI DEC 22 2000 15:32:52 UTC)
NOTICE 01/10/2001 00:59:52 os: last reset: user reboot, reason: not specified
NOTICE 01/10/2001 00:59:52 os: OsIsrRegistrar: 0xb
NOTICE 01/10/2001 00:59:52 os: OsIsrRegistrar: 0xa
NOTICE 01/10/2001 00:59:52 os: OsIsrRegistrar: 0x2
```

- By combining keywords, you can further limit the information displayed. See the CLI online Help for information about the keywords available at each level.

```
host1#show log data nv-file severity alert
```


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.

aaaAtm1483Cfg

Description	AAA ATM 1483 subinterface configuration
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Illegal service category traffic parameter received from AAA; unable to modify circuit traffic parameters using those received from AAA
Notice Log	None
Info	None
Debug	Notification from AAA indicating that an ATM 1483 subinterface configuration is available; ATM 1483 processing configuration received from AAA; unable to get ATM 1483 subinterface information; number of ATM 1483 configuration entries is out of range
Filter	None

aaaEngineGeneral

Description	AAA engine general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Control flow and key events, less verbose than debug
Info	None
Debug	Control flow and key events
Filter	None

aaaQosCfg

Description	AAA QoS configuration logs
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	AAA QoS configuration tracking
Filter	None

aaaServerGeneral

Description	AAA server general
Emergency	None
Alert	None
Critical	None
Error	Subscriber count exceeds license plus grace; internal attachment errors
Warning Log	Subscriber count exceeds license; cannot grow internal memory pools; accounting message failures
Notice Log	Authentication failures resulting from memory allocation failures
Info	None
Debug	Authentication failures resulting from reasons other than memory allocation failures; status of authentication; accounting and address assignment requests sent to local (internal) servers; duplicate accounting message failures; EAP challenge received
Filter	None

aaaUserAccess

Description	AAA user access
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	User is granted or denied access
Debug	None
Filter	None

addressServerGeneral

Description	Address server general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Address server request failure (for example, configured address server is not available)
Notice Log	None
Info	None
Debug	None
Filter	None

ar1AaaServerGeneral

Description	Platform-dependent AAA server
Emergency	None
Alert	None
Critical	None
Error	Internal (NVS) errors for limit configuration per interface
Warning Log	None
Notice Log	None
Info	None
Debug	Interface information insufficient to identify the user's interface location
Filter	None

atm

Description	ATM interface
Emergency	None
Alert	None
Critical	None
Error	Unable to reenable ILMI administrative state after UNI version change
Warning Log	Error getting location of underlying physical interface; error binding or unbinding to physical interface; error allocating memory for new interface; error setting system identifier; error adding or configuring an interface; error getting capabilities of interface; error getting maximum VPI/VCI for interface; error getting maximum virtual circuit descriptor for interface; unable to store or allocate memory for F4 OAM circuit data; unable to configure F4 OAM circuit for interface
Notice Log	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
Info	Dropping interface up, down, or not present notification due to removal of interface; discarding F4 OAM circuits when interface does not support F4 OAM
Debug	None
Filter	None

atm1483

Description ATM 1483 data service**Emergency** None**Alert** None**Critical** None**Error** 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**Warning Log** 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**Notice Log** 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**Info** 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**Debug** None**Filter** None

atm1483VcClass

Description	Application of attributes configured in a virtual circuit (VC) class to PVCs
Emergency	None
Alert	None
Critical	None
Error	In routers with high availability enabled, failure to mirror the VC modification or failure to associate the VC modification with the standby SRP module
Warning Log	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
Notice Log	None
Info	None
Debug	None
Filter	None

atmAal5

Description	ATM Adaptation Layer 5
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	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
Notice Log	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
Info	Dropping interface up or down notification due to removal of interface
Debug	None
Filter	None

atmVcClass

Description	Information on VC class operational errors
Emergency	None
Alert	None
Critical	None
Error	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
Warning Log	None
Notice Log	None
Info	None
Debug	Unable to update mirrored storage for a high availability switchover
Filter	None

auditIpsec

Description	IKE SA negotiations
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Information about IKE SA negotiation payloads
Info	None
Debug	None
Filter	None

bfdAdaptivity

Description	BFD adaptivity events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	BFD session adaptivity events
Debug	BFD session adaptivity events
Filter	None

bfdEvents

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

bfdGeneral

Description	BFD general events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	BFD enabled/disabled on an interface from a client
Info	None
Debug	None
Filter	None

bfdSession

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

bgpConnections

Description	BGP TCP/IP connection activity
Emergency	None
Alert	None
Critical	None
Error	Error setting password for specified peer; error binding to update-source address for specified peer
Warning Log	TCP error occurred while receiving data
Notice Log	Outbound TCP connection initiated, completed, or failed; inbound TCP connection accepted, refused, or failed; TCP connection closed by peer
Info	None
Debug	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
Filter 1:	access-class—This filter is not currently supported
Filter 2:	peer—See description of the bgpRoutes peer filter for information about this filter
Filter 3:	route-map—This filter is not currently supported
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

bgpDampening

Description	BGP dampening
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Route is suppressed by route-flap dampening; route is no longer suppressed by route-flap dampening
Info	None
Debug	None
Filter 1:	access-class—This filter is not currently supported
Filter 2:	peer—See description of the bgpRoutes peer filter for information about this filter
Filter 3:	route-map—This filter is not currently supported
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

bgpEvents

Description	BGP finite state machine (FSM) events and transitions
Emergency	None
Alert	None
Critical	None
Error	Event occurred that was not expected for current state
Warning Log	None
Notice Log	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
Info	None
Debug	None
Filter 1:	access-class—This filter is not currently supported
Filter 2:	peer—See description of the bgpRoutes peer filter for information about this filter
Filter 3:	route-map—This filter is not currently supported
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

bgpGeneral

Description	BGP general information
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	BGP IPv4 route-target-signaling address family enabled or disabled
Info	None
Debug	None
Filter 1:	access-class—This filter is not currently supported
Filter 2:	peer—See description of the bgpRoutes peer filter for information about this filter
Filter 3:	route-map—This filter is not currently supported
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

bgpGracefulRestart

Description	BGP Graceful Restart Feature log
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	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
Info	None
Debug	Standby SRP will wait for BGP convergence on next restart
Filter 1:	access-class—This filter is not currently supported
Filter 2:	peer—This filter is not currently supported
Filter 3:	route-map—This filter is not currently supported
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

bgplpv6NextHops

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

bgpKeepAlives

Description	BGP keepalive messages
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Keepalive message received with unexpected additional data after header
Notice Log	Keepalive message received; keepalive message sent
Info	None
Debug	None
Filter 1:	access-class—This filter is not currently supported
Filter 2:	peer—See description of the bgpRoutes peer filter for information about this filter
Filter 3:	route-map—This filter is not currently supported
Filter 4:	router—See description of the bgpRoutes router filter for information about this filter
Filter 5:	in—Matches on traffic coming into the router
Filter 6:	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

Description	BGP protocol messages
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	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
Notice Log	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
Info	None
Debug	Keepalive message received or sent (Full decode of message logged if verbosity is high).



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

- Filter 1:** access-class—This filter is not currently supported
- Filter 2:** peer—See description of the bgpRoutes peer filter for information about this filter
- Filter 3:** route-map—This filter is not currently supported
- Filter 4:** router—See description of the bgpRoutes router filter for information about this filter
- Filter 5:** in—Matches on traffic coming into the router
- Filter 6:** out—Matches on traffic going out of the router

bgpNeighborChanges

Description	BGP neighbor change
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	A peer has entered into or left the established state; reason for a session going idle
Info	None
Debug	None
Filter 1:	access-class—This filter is not currently supported
Filter 2:	peer—See description of the bgpRoutes peer filter for information about this filter
Filter 3:	route-map—This filter is not currently supported
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

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

bgpRoutes

Description	BGP routing table updates
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Failure to add, remove, or modify BGP route in IP forwarding table
Notice Log	BGP route added to, removed from, or modified in the IP forwarding table; aggregate route added to, removed from, or modified in Loc-RIB; network route added to, removed from, or modified in Loc-RIB; best route for internal peers for a given prefix became available; best route for internal peers for a given prefix is no longer available, has changed, or has become available; best route for external peers for a given prefix is no longer available, has changed, or has become available; MPLS base tunnel used to reach an indirect next-hop came up or went down; MPLS stacked tunnel for label came up; indirect next-hop became reachable or unreachable; direct next-hop for an indirect next-hop changed; MPLS tunnel for Inter-AS label came up or went down; route added to L2VPN instance; route deleted from L2VPN instance; route modified for L2VPN instance
Info	None
Debug	Redistributed route added to, removed from, or modified in Loc-RIB; advertisement for a given prefix received; withdraw for a given prefix received; local route-target-filtering route added to or removed from <i>prefix</i> in <i>addressFamily</i>
Filter 1:	<p>access-class <i>accessClassName</i> [route-map <i>routeMapName</i> <i>routeMapOptions</i> filtering-router <i>filteringRouterName</i> <i>filteringRouterOptions</i> in out]</p> <ul style="list-style-type: none"> ■ access-class—Logs events for traffic that matches a specific access class ■ <i>accessClassName</i> —Name of the access class for which you want to log events ■ route-map—Logs events for traffic that matches a specific route map ■ <i>routeMapName</i>—Name of route map for which you want to log events ■ <i>routeMapOptions</i>—In the following format—filtering-router <i>filteringRouterName</i> <i>filteringRouterOptions</i> in out ■ filtering-router—Logs events only if the access class or route map are defined on a specific virtual router ■ <i>filteringRouterName</i>—Virtual router where the access class or route map or both are defined ■ <i>filteringRouterOptions</i>—in out

- in—Matches on traffic coming into the access class, route map, or virtual router
- out—Matches on traffic sent out of the access class, route map, or virtual router

Filter 2: `peer peerIpAddress | peerIpv6Address`
`[access-class accessClassName accessClassOptions |`
`route-map routeMapName routeMapOptions |`
`filtering-router filteringRouterName filteringRouterOptions | in | out]`

- peer—Logs events for traffic that matches a specific peer
- *peerIpAddress*—IP address of the peer for which you want to log events
- *peerIpv6Address*—IPv6 address of the peer for which you want to log events
- access-class—Logs events for traffic that matches a specific access class
- *accessClassName*—Name of the access class for which you want to log events
- *accessClassOptions*—In the following format—`filtering-router filteringRouterName filteringRouterOptions | in | out`
- route-map—Logs events for traffic that matches a specific route map
- *routeMapName*—Name of route map for which you want to log events
- *routeMapOptions*—In the following format—`filtering-router filteringRouterName filteringRouterOptions | in | out`
- filtering-router—Logs events only if the peer, access class or route map are defined on a specific virtual router
- *filteringRouterName*—Virtual router where the peer, access class or route map or both are defined
- *filteringRouterOptions*—in | out
- in—Matches on traffic coming into the peer, access class, route map, or virtual router
- out—Matches on traffic sent out of the peer, access class, route map, or virtual router

Filter 3: `route-map routeMapName`
`[filtering-router filteringRouterName filteringRouterOptions | in | out]`

- route-map—Logs events for traffic that matches a specific route map
- *routeMapName*—Name of route map for which you want to log events
- filtering-router—Logs events only if the route map is defined on a specific virtual router
- *filteringRouterName*—Virtual router where the route map is defined

- *filteringRouterOptions*—in | out
- in—Matches on traffic coming into the route map or virtual router
- out—Matches on traffic sent out of the route map or virtual router

Filter 4: router *virtualRouterName* [access-class *accessClassName* *accessClassOptions* | route-map *routeMapName* *routeMapOptions* | filtering-router *filteringRouterName* *filteringRouterOptions* | peer *peerIpAddress* *peerOptions* | in | out]

- router—Logs events for traffic on a specific virtual router
- *virtualRouterName*—Name of virtual router
- access-class—Logs events for traffic that matches a specific access class on the specified router
- *accessClassName*—Name of the access class for which you want to log events
- *accessClassOptions*—In the following format—route-map *routeMapName* *routeMapOptions* | virtual-router *virtualRouterName* *virtualRouterOptions* | in | out
- route-map—Logs events for traffic that matches a specific route map
- *routeMapName*—Name of route map for which you want to log events
- *routeMapOptions*—In the following format—virtual-router *virtualRouterName* *virtualRouterOptions* | in | out
- filtering-router—Logs events only if the access class or route map is defined on a specific virtual router
- *filteringRouterName*—Virtual router where the access class or route map is defined
- *filteringRouterOptions*—In the following format—in | out
- peer—Logs events for traffic that matches a specific peer
- *peerIpAddress*—Address of the peer for which you want to log events
- *peerOptions*—In the following format—access-class *accessClassName* *accessClassOptions* | filtering-router *filteringRouterName* *filteringRouterOptions* | route-map *routeMapName* *routeMapOptions* | in | out
- in—Matches on traffic coming into the virtual router, access class, or route map
- out—Matches on traffic sent out of the virtual router, access class, or route map

Filter 5: in—Matches on traffic coming into the router

Filter 6: out—Matches on traffic going out of the router

bridge

Description	Bridge group configuration
Emergency	None
Alert	None
Critical	None
Error	Bridge interface, learning, aging, and static MAC address errors
Warning Log	Bridge resources (maximum interfaces, memory exhaustion)
Notice Log	Bridge group interface location availability, operation status, and MTU changes
Info	Bridge group state changes (start, shutdown); bridge interface, learning, aging, and static MAC address modifications
Debug	Verbose bridge interface, learning, aging, and static MAC address configuration and status
Filter	None

bridgeEngine

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

bridgingMgr

Description	Bridging manager configuration
Emergency	None
Alert	None
Critical	None
Error	Bridge mode, bridge group, and subscriber policy errors
Warning Log	Bridging manager resources (maximum bridge groups, maximum subscriber policies, memory exhaustion)
Notice Log	None
Info	Bridging manager operation state changes (init, start, shutdown); bridge mode, bridge group, and subscriber policy modifications
Debug	Verbose bridge mode, bridge group, and subscriber policy configuration and status
Filter	None

bulkStats

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

cacGeneral

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

cacIntf

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



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

cliCommand

Description	CLI commands
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	All successful CLI configuration commands
Info	All unsuccessful CLI configuration commands; all nonconfiguration commands
Debug	None
Filter	None

cliGeneral

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

connectionManager

Description	Logging various conditions in the component that manages the chassis fabric.
Emergency	None
Alert	None
Critical	10G and 5G SRP modules only—Detection that the FPGAs have not been loaded (results in an SRP [and chassis] reset)
Error	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.
Warning Log	Cannot connect to a particular source or destination address (board may have just been removed)
Notice Log	A connection that previously could not be closed has now closed; a multicast destination that previously could not be dropped has now been dropped
Info	Various logs to indicate events and transitions for low level diagnosis
Debug	Various logs to indicate events and transitions for low level diagnosis
Filter	None

cops

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

copsPr

Description	COPS-PR general log
Emergency	None
Alert	None
Critical	None
Error	Error decoding COPS-PR messages received from the SDX program
Warning Log	Outstanding COPS-PR pool allocations while attempting to shut down SSC client; temporary resource allocations while sending COPS-PR messages to SDX program
Notice Log	None
Info	None
Debug	None
Filter	None

coreDump

Description	Core dump events
Emergency	None
Alert	None
Critical	None
Error	Connection errors; file open errors; write failures; core dump failures; transfer errors
Warning Log	Core dump configuration changes due to core dump monitor; core dump monitor memory allocation errors
Notice Log	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
Info	None
Debug	lcLoader creation; dump request receipt; core dump monitor start; core dump monitor stop
Filter	None

ctreeLog

Description	For internal maintenance of IP routes
Emergency	None
Alert	None
Critical	None
Error	Failure in insertion, deletion, and update of IP routes in internal data structure used to maintain the routes
Warning Log	None
Notice Log	None
Info	None
Debug	Creation or deletion of an internal data structure
Filter	None

dcm

Description	Dynamic Configuration Manager
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	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
Filter	None

dcmEngineGeneral

Description	DCM engine general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Giving notify credits to line module; receipt of request buffer from line module; starting line module communication session; Ack/Nack dynamic interface creation request
Filter	None

dhcpCapture

Description	DHCP packet capture
Emergency	None
Alert	None
Critical	None
Error	
Error	Configuration errors
Warning Log	Processing errors (resource exhaustion)
Notice Log	None
Info	Logged DHCP packets, configured by the ip dhcp-capture command (specify high verbosity for detail)
Debug	Configuration change details; DHCP discover, offer, request, decline, and ACK/NAK packets on a per-interface basis
Filter	None

dhcpExternal

Description	DHCP external
Emergency	None
Alert	None
Critical	None
Error	Configuration errors; client processing errors (invalid data)
Warning Log	Client processing errors (resource exhaustion)
Notice Log	Configuration changes
Info	None
Debug	Configuration change details; client events
Filter	None

dhcpExternalEngine

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

dhcpGeneral

Description	DHCP general
Emergency	None
Alert	Rvn8
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	DHCP message received
Filter	None

dhcplssuLog

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

dhcpLocalClients

Description	DHCP local server clients
Emergency	None
Alert	None
Critical	None
Error	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
Warning Log	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, using DHCP values; secondary NetBIOS Name Server (NBNS) without primary NBNS configured, using DHCP values
Notice Log	None
Info	None
Debug	Removing stale offers to clients and stale clients; adding and removing clients; expiring client's lease; client's transactions with DHCP local server
Filter	None

dhcpLocalGeneral

Description	General DHCP local server
Emergency	None
Alert	None
Critical	None
Error	Memory allocation failure; cannot find interface location for the UID
Warning Log	No DHCP instance to process the received packet; hard limits reached; packet discarded due to no resources
Notice Log	DHCP local server not configured; client's session failed to start
Info	Client per-interface limit exceeded; client per-interface exceeded condition abated
Debug	Any log message that indicates the status of the general operation of the DHCP local server; NVS actions; grace period lease state; configuration changes
Filter	None



NOTE: This category replaces the dhcpLocalServerGeneral category.

dhcpLocalHighAvailability

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

dhcpLocalPool

Description	DHCP local address pool, including normal, linked, and shared pools
Emergency	None
Alert	Local pool IP address is exhausted (address limit violation)
Critical	Higher limit of address pool utilization reached
Error	None
Warning Log	Lower limit of address pool utilization reached; invalid DHCP local address pool attributes
Notice Log	None
Info	None
Debug	DHCP local address pool resolution; address allocation
Filter	None

dhcpLocalProtocol

Description	DHCP local server protocol
Emergency	None
Alert	None
Critical	None
Error	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
Warning Log	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
Notice Log	None
Info	None
Debug	Received packet; transmit packet; authentication status; DHCP local server state transitions
Filter	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> ■ interface—Logs events for a specific interface ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

dhcpNvGeneral

Description	DHCP host route preservation
Emergency	None
Alert	None
Critical	None
Error	Null interface for DHCP clients
Warning Log	None
Notice Log	None
Info	Output from VxWorks shell “dhcp-NvShow” command
Debug	NVS cache creation; entries added to or removed from the cache; cache synchronized to NVS
Filter	None

dhcpOfferLog

Description	DHCP offer selection process log
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Status of the offer selection process
Filter	None

dhcpPbeGeneral

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

dhcpProxyGeneral

Description	DHCP Proxy general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Control flow and key events
Filter	None

dhcpRelayGeneral

Description	DHCP Relay general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	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
Filter	None

dhcpv6Client

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

dhcpx6DemuxGeneral

Description	DHCPv6 packet demultiplexer events
Emergency	None
Alert	None
Critical	None
Error	UDP transmit errors, out-of-memory conditions, internal errors
Warning Log	Invalid DHCPv6 packet type received
Notice Log	None
Info	None
Debug	None
Filter	None

dhcpx6LsGeneral

Description	DHCPv6 local server events
Emergency	None
Alert	None
Critical	None
Error	Failure to create server (bad router or out of memory)
Warning Log	Attempt to remove a nonexistent server
Notice Log	Failure to create server (IPv6 not licensed)
Info	None
Debug	Server bind, creation, deletion, and unbind
Filter	None

dismanEventMgr

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

dnsGeneralLog

Description	DNS general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Failure to post a message to DNS about the query response from DNS server
Notice Log	None
Info	None
Debug	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
Filter	None

dosProtection

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

ds1

Description	DS1 layer
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Interface creation or binding failure
Notice Log	Failure to bring line module application online; dropped interface state change notification due to lack of resources; discarded stale line module notification
Info	Dropped interface state change notification for unknown or removed interface
Debug	None
Filter	None

ds3

Description	DS3 layer
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Failure to create or bind interface
Notice Log	Failure to bring line module application online; dropped interface state change notification due to lack of resources; discarded stale line module notification
Info	Dropped interface state change notification for unknown or removed interface
Debug	None
Filter	None

dvmrpGeneral

Description	DVMRP general
Emergency	None
Alert	None
Critical	None
Error	Memory allocation errors; bad parameters (internal errors); designated forwarder errors (two for same interface, DoNotForward by no designated forwarder); processing prune errors; graft errors; internal errors; catastrophic RT table errors; management interaction errors; NVS errors
Warning Log	Unable to add local route; routeHogCheck; routeLimit
Notice Log	Route expiration; pruneProcessing (send or receive); graftAck processing; source group (SG) state information; deletion of an output interface; nbrQuickDelete; nbrReset; nbrTimeOut; error adding neighbor on Route Report Reception
Info	Designated forwarder election information; sending graft; timer expired for MulticastEntry; attempting to log duplicate accept filter; external route deleted or added
Debug	Local address creation or deletion; information about accept filters; dvmrpInterface creation or deletion; sgTimeout information; noMoreOifs info; sg creation information; multicastForwarding enabled or disabled; DvmrpInit; dvmrpEnable/Disable; rpfCallback

Filter 1: `interface interfaceType interfaceSpecifier`

- `interface`—Logs events for a specific interface
- `interfaceType`—Type of interface for which you want to log events
- `interfaceSpecifier`—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: `router virtualRouterName [interface interfaceType interfaceSpecifier]`

- `router`—Logs events for a specific virtual router
- `virtualRouterName`—Name of virtual router for which you want to log events
- `interface`—Logs events on a specific interface on the virtual router
- `interfaceType`—Type of interface for which you want to log events
- `interfaceSpecifier`—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

dvmrpGracefulRestart

Description	DVMRP graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	DVMRP graceful restart complete
Info	None
Debug	None
Filter	None

dvmrpMcastTable

Description	DVMRP multicast table messages
Emergency	None
Alert	None
Critical	None
Error	Error removing MulticastEntry; adding duplicate MulticastEntry; adding nonexistent MulticastEntry; attempting to send prune to nonexistent neighbor; error deleting MulticastEntry; error adding outgoing interfaces
Warning Log	Deleting MulticastEntry with no SG state found; attempting to create MulticastEntry, but unable to do so
Notice Log	Creating MulticastEntry
Info	rePruning; delOif; add outgoing interface; not adding outgoing interface for some reason; creating sgoiflist; pruneDelayCallback; prune; deleting MulticastEntry
Debug	None
Filter 1:	interface—See description of the dvmrpGeneral interface filter for information about this filter
Filter 2:	router—See description of the dvmrpGeneral router filter for information about this filter

dvmrpProbeRcv

Description	DVMRP probe received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	procProbe new neighbor
Info	None
Debug	Processing probe (verified has our address in packet); display probe
Filter 1:	interface—See description of the dvmrpGeneral interface filter for information about this filter
Filter 2:	router—See description of the dvmrpGeneral router filter for information about this filter

dvmrpProbeSent

Description	DVMRP probe sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Send probe
Filter 1:	interface—See description of the dvmrpGeneral interface filter for information about this filter
Filter 2:	router—See description of the dvmrpGeneral router filter for information about this filter

dvmrpRtTable

Description	DVMRP Routing Table
Emergency	None
Alert	None
Critical	None
Error	Route error; router report error; error replacing route after applying accept filter; internal errors
Warning Log	Unable to create new route; deleting routing table
Notice Log	Error in report packet; adding or replacing local route; ignoring poison on upstream user interface (USIF); deleting all dependent neighbors
Info	Processing report; added route from report; declaring ourselves as designated forwarder; route update
Debug	Delete route; insert route
Filter 1:	interface—See description of the dvmrpGeneral interface filter for information about this filter
Filter 2:	router—See description of the dvmrpGeneral router filter for information about this filter

ethernet

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

ethernetStateSession

Description	Configuration of the Fast Ethernet management port on the SRP IOA on the E320 router or the E120 router
Emergency	None
Alert	None
Critical	None
Error	Configuration errors for duplex mode and speed settings on the Fast Ethernet management port
Warning Log	Configuration did not occur for duplex mode and speed on the Fast Ethernet management port
Notice Log	None
Info	None
Debug	None
Filter	None

fileSystem

Description	File system
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Missing of invalid armed files
Notice Log	None
Info	None
Debug	Timestamp of last synchronization
Filter	None

flowInspection

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

flowInspectionEngine

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

flowServicesFirewallAlert

Description	Firewall
Emergency	None
Alert	None
Critical	None
Error	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
Warning Log	None
Notice Log	Oldest entry deleted; rate of connections has decreased to the specified limit; number of connections has decreased to below the specified limit
Info	None
Debug	None
Filter	None

flowServicesFirewallAudit

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

frameRelay

Description	Frame Relay layer
Emergency	None
Alert	None
Critical	Failure to bring up the application due to lack of memory resources
Error	Summary information about automatic removal of interface or circuit from nonvolatile storage on startup; internal resource pool is too small
Warning Log	None
Notice Log	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
Info	Line module insertion and removal information
Debug	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
Filter	None

fsAgent

Description	File System Agent
Emergency	None
Alert	None
Critical	Previous file system sync failed—booting protected images
Error	File system unavailable
Warning Log	File transfer initialization failure; unexpected software error
Notice Log	None
Info	File transfer notification; platform or release mismatch; file transfer error; release file is corrupt; image path not found; insufficient resources to copy release
Debug	Status of copy running-config; file transfer status; backup boot-setting configuration notification; subsystem release configuration notification
Filter	None

ft1

Description	FT1 layer
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Interface creation or binding failure
Notice Log	Failure to bring line module application online; dropped interface state change notification due to lack of resources; discarded stale line module notification
Info	Dropped interface state change notification for unknown or removed interface
Debug	None
Filter	None

ftpClient

Description	FTP client
Emergency	None
Alert	None
Critical	None
Error	Unexpected results during a transfer
Warning Log	None
Notice Log	Completion status of a network connection command (example: "Succeeded creating data socket")
Info	Completion status of a user command (example: "LS command succeeded")
Debug	None
Filter	None

ftpServer

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

gplaan

Description	General purpose locally allocated address notifier
Emergency	None
Alert	None
Critical	None
Error	Out of resources
Warning Log	None
Notice Log	Task creation or deletion
Info	None
Debug	Adding or deleting IP addresses; adding or deleting user sessions
Filter	None

ha

Description	High availability messages
Emergency	None
Alert	None
Critical	None
Error	Accessing redundancy mode is not supported on the standby SRP; changing redundancy mode is not supported on the standby SRP; high availability disabled due to state error
Warning Log	High availability disabled due to incompatible release on standby; high availability disabled due to user initiated disable
Notice Log	High availability disabled due to standby down; high availability is now active
Info	None
Debug	None
Filter	None

hdlc

Description	HDLC layer
Emergency	None
Alert	None
Critical	None
Error	Interface creation failures (interface is not created); interface configuration errors; interface pool failures
Warning Log	Interface creation failures during initialization; interface deletion failures (interface is still deleted); interface pool failures (might not cause problems)
Notice Log	Interface pool changes
Info	Layer initialization messages; interface creation; interface modification; interface deletion
Debug	Detailed layer initialization; interface creation details; interface deletion details
Filter	None

hotfixGeneral

Description	Hotfix general
Emergency	None
Alert	None
Critical	None
Error	Error conditions causing startup hotfix activation to fail
Warning Log	Failed to deactivate or disarm a hotfix; attempts to activate incompatible hotfixes
Notice Log	Activation or arming of a hotfix
Info	None
Debug	None
Filter	None

httpServer

Description	Embedded HTTP server
Emergency	None
Alert	None
Critical	None
Error	Failure to enable HTTP daemons (httpd); failure to remove httpd; failure to grow pool of httpds or pool of HTTP connections (httpcs); failure to listen on httpd socket; failure to set TCP socket options; failure to remove TCP socket; failure to queue HTTP event (socket accept, socket approve, socket send, socket receive); failure to queue HTTP event for maximum connection aging; invalid HTTP event
Warning Log	Refused HTTP connection due to too many simultaneous connections from same host; refused HTTP connection due to access list deny; failure to perform TCP socket approval; failure to send data on TCP socket
Notice Log	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 (httpcs); 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 gplanDelete; 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 httpcs; 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

iclImageFixServer

Emergency	None
Alert	None
Critical	None
Error	Memory allocation failure; ImageFix load failure; manual ImageFix activation failure; ImageFix file errors
Warning Log	Buffer allocation failure; unexpected status received in state X
Notice Log	Application image up, startup ImageFixes activated; reversion from FC ImageFix to release FC image requires reload of line module; FC ImageFix found for line module
Info	State machine change; unexpected internal communication error; loading complete announcement; IC up-to-date following SRP switch; sending ImageFix descriptor to line module
Debug	Controller state change announcement; board state change announcement; manual ImageFix [de]activation attempt; subsystem announced
Filter	None

icmpTraffic

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

icmpv6Traffic

Description	ICMPv6 frame transmit or receive
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Packets of unknown types, invalid headers, with header errors
Notice Log	None
Info	Failures due to checksum errors, unsupported
Debug	All ICMPv6 transmit or receive events
Filter 1:	[remote-ipv6-address <i>ipv6Address</i>]
	<ul style="list-style-type: none"> remote-ipv6-address—Logs events for packets arriving from or going to a specified IPv6 address <i>ipv6Address</i>—IPv6 address of remote system for which you want to log messages
Filter 2:	router <i>virtualRouterName</i> [address <i>ipv6Address</i>]
	<ul style="list-style-type: none"> router—Logs events on a specific virtual router <i>virtualRouterName</i>—Name of virtual router for which you want to log events address—Logs events on a specific IPv6 address <i>ipv6Address</i>—Address of remote system for which you want to log messages

igmpGeneral

Description	IGMP general
Emergency	None
Alert	None
Critical	None
Error	Nonrecoverable errors
Warning Log	NVS errors
Notice Log	Errors while configuring or learning groups
Info	None
Debug	IGMP interface or group state change; errors in packet transmit or receive
Filter 1:	interface <i>interfaceType interfaceSpecifier</i> <ul style="list-style-type: none"> ■ interface—Logs events for a specific interface ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2:	router <i>virtualRouterName</i> [interface <i>interfaceType interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ interface—Logs events on a specific interface on the virtual router ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format
------------------	---



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

igmpGracefulRestart

Description	IGMP graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	IGMP/MLD graceful restart complete
Info	None
Debug	None
Filter	None

igmpGroupState

Description	IGMP group state change events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	igmp v2 first host join, last host leave events (Release 5.0 and earlier); igmp v3 state change and source-list change events aggregated across all hosts on the interface (Release 5.1.0 and later)
Debug	None
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events ■ interface—Logs events on a specific interface on the virtual router ■ <i>interfaceType</i>—Type of the interface for which you want to log events. For example, atm or fastEthernet. ■ <i>interfaceSpecifier</i>—Location of the interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

ikeCertificateMgr

Description	Displays events relating to ERX key generation, certificate status, and certificate processing
Emergency	None
Alert	None
Critical	None
Error	Initialization problems
Warning Log	Missing ERX private key; public key does not match private key; certificate expired; memory allocation problems; CRL too large; attempt to generate new key pair before deleting old one; key generation problems; problem reading private key
Notice Log	Problem decoding certificates; IKE authentication problems related to certificates
Info	None
Debug	Certificate database notifications
Filter	None

ikeEnrollment

Description	Displays events relating to certificate enrollment
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Identity no set; missing ERX private key; missing CA certificate; enrollment failures
Notice Log	None
Info	Received CA certificate; received CA and RA certificate chain; received ERX certificate; retry scep poll message
Debug	Found CA certificate; found ERX certificates; enrollment failure details
Filter	None

ikepki

Description	IKE SA negotiation
Emergency	None
Alert	None
Critical	None
Error	Event occurred that is unexpected for the current state
Warning Log	Memory pool growth problems; recoverable state problems; receiving IKE packets for unconfigured peer
Notice Log	IKE configuration problems—no preshared keys for peer; recoverable status conditions
Info	Number of successful SAs negotiation, both phase 1 and phase 2; unsuccessful phase 1 negotiation information; unsuccessful phase 2 negotiation information
Debug	Detailed SA negotiation debug information
Filter	None

interModuleCommunication

Description	Intermodule communication monitoring
Emergency	None
Alert	None
Critical	Line card resetting after recovery attempts fail; standby SRP resetting after monitoring thresholds exceeded
Error	None
Warning Log	Line card recovery attempts after monitoring thresholds exceeded
Notice Log	Ping monitoring threshold exceeded; ICC session monitoring threshold exceeded; ICC connection monitoring threshold exceeded
Info	Intermodule communication monitoring condition, state change, and corresponding action
Debug	None
Filter	slot <i>slotNumber</i> <ul style="list-style-type: none"> ■ slot—Logs events for a specific slot ■ <i>slotNumber</i>—Number of slot for which you want to log events

ipAccessList

Description	IP access list matching
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Access list rule has been matched
Debug	None
Filter 1:	accessList <ul style="list-style-type: none"> ■ accessList—Logs a match on any access-list entry for all access lists
Filter 2:	accessList router <i>virtualRouterName</i> access-list <i>accessListName</i> access-element-id <i>idNumber</i> <ul style="list-style-type: none"> ■ accessList—Logs a match on any access-list entry ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ access-list—Logs events for a specific access list ■ <i>accessListName</i>—Name of access list for which you want to log events ■ access-element-id—Logs events for a specific element ID ■ <i>idNumber</i>—Element ID number for which you want to log events; the element ID is automatically assigned for access-list rules that you explicitly create and is shown by issuing the show access-list detail command

ipEngine

Description	IP chassis manager
Emergency	None
Alert	None
Critical	None
Error	Failure in operations such as adding, removing, or deleting interfaces or distributing routing tables to line modules
Warning Log	Errors such as attempting to configure something that is not supported on a module, or routing table memory is approaching 80 percent full
Notice Log	Something unexpected happened; for example, an interface was deleted twice or, internal to the software, connections between IC and SRP were deleted twice
Info	Completion status of a user command (for example: "IS command succeeded")
Debug	An engine or agent that corresponds to a virtual router is added or deleted; an interface is added or deleted
Filter	None

ipflowstats

Description	J-Flow statistics
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Application starting
Info	Interfaces become available or unavailable
Debug	Main and History cache tables are cleared
Filter	None

ipflowstatsEngine

Description	J-Flow statistics engine
Emergency	None
Alert	None
Critical	None
Error	Agents stopping or deleting; memory allocation errors; line module errors
Warning Log	Problems bring modules or slots up or down
Notice Log	None
Info	Agent or master creation; slot or operation state information
Debug	Creation or removal of engine; initialization problems
Filter	None

ipGeneral

Description	IP general
Emergency	None
Alert	None
Critical	(IP) Interface stacking management errors
Error	(ARP) Allocation of Ethernet next hop failed (IP) Not able to create interface or create address on null 0 interface; undefined IP status code; interface stacking management errors; send and forward failures because of not finding corresponding egress or ingress nodes; conflict in adding hidden routes
Warning Log	(IP) NVS load errors; failure to add address on an interface because of low memory
Notice Log	None
Info	None
Debug	(ARP) NextHopPool is out of memory and trying to expire old entries; ARP data events (IP) Interface stacking management errors

Filter 1: interface *interfaceType* *interfaceSpecifier*

- interface—Logs events for a specific interface
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName* [interface *interfaceType* *interfaceSpecifier*]

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



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

ipIfCreator

Description	IP interface creator events
Emergency	None
Alert	None
Critical	None
Error	Out of resources failures in midoperation; client application and DCM interaction errors (out-of-range sessionId or enum; unrecognized message type); failure during client callback for interface creation
Warning Log	Client session already unbound; unable to process new configuration requests (out of resources)
Notice Log	Interface deletion failure in DCM (no client acknowledgement required)
Info	None
Debug	Client interaction during bind or unbind, session creation or shutdown, and interface creation or deletion; DCM interaction during interface creation or deletion
Filter	None

ipInterface

Description	IP interface
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Error status is returned by lower layer configuration; best route is pointing to an unnumbered interface with an invalid source IP address; unnumbered interface is pointing to invalid loopback interface problems; packets received with invalid source IP address on interfaces
Notice Log	None
Info	None
Debug	Interface state transitions and deletions; interface state machine events
Filter 1:	interface—See description of the ipGeneral interface filter for information about this filter
Filter 2:	router—See description of the ipGeneral router filter for information about this filter

ipNhopTrackerGeneral

Description	Next-hop tracker for IP shared interfaces
Emergency	None
Alert	None
Critical	None
Error	Errors in tracking of routes that resolve indirect next hops
Warning Log	None
Notice Log	None
Info	None
Debug	None
Filter	None

ipProfileMgr

Description	IP Profile Manager
Emergency	None
Alert	None
Critical	None
Error	Failure to create or delete dynamic IP interfaces
Warning Log	None
Notice Log	None
Info	None
Debug	Events related to dynamic IP interface creation or deletion; assignment or unassignment of profiles to interfaces
Filter	None

ipRoutePolicy

Description	IP route policy
Emergency	None
Alert	None
Critical	None
Error	Failure to clean up NVS while a routing policy was being deleted; failure to store the routing policy to NVS while a new routing policy was being created; failure to find an expected routing policy created previously
Warning Log	Failure to create a new routing policy due to memory limitation; misuse of a routing policy
Notice Log	None
Info	Result of routing policy check; specifies which routing policy is used
Debug	Successful addition or deletion of routing policies
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs IP route policy events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

ipRouteTable

Description	IP routing table
Emergency	None
Alert	None
Critical	None
Error	Next-hop resolution-related problems; exceeding maximum route limit or warning threshold
Warning Log	Failure to add route
Notice Log	None
Info	In process of finding best route information
Debug	Normal routing table updates; next-hop resolution for static routes
Filter 1:	interface—See description of the ipGeneral interface filter for information about this filter
Filter 2:	router—See description of the ipGeneral router filter for information about this filter

ipseclDb

Description	Phase 1 identity database information. Used for deciding which phase 1 identity to use for incoming IKE negotiations.
Emergency	None
Alert	None
Critical	None
Error	Internal dBase issue with hashes
Warning Log	Problems adding or deleting entries
Notice Log	None
Info	Adding entries to database
Debug	Detailed database information and transactions
Filter	None

ipsecP1Throttler

Description	Ongoing phase 1 negotiations
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Throttling instances based on suspicious flows (for example, the same peer failing repeated fast negotiations)
Notice Log	None
Info	None
Debug	None
Filter	None

ipsecXcfgSM

Description	Xauth application state machine information.
Emergency	None
Alert	None
Critical	None
Error	Internal state machine errors
Warning Log	State machine unexpected events; problems with xauth negotiations
Notice Log	Significant state changes
Info	None
Debug	None
Filter	None

ipSubscriberMgr

Description	IP Subscriber Manager
Emergency	None
Alert	None
Critical	None
Error	Primary interface not found
Warning Log	None
Notice Log	None
Info	None
Debug	Dump parameters for methods; dump results for lookups; dump points during thread execution.
Filter	None

ipTraffic

Description	IP frame transmit and receive
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Data errors detected in frames
Notice Log	Dropped frames—No error
Info	None
Debug	Normal data events
Filter 1:	interface—See description of the ipGeneral interface filter for information about this filter
Filter 2:	router—See description of the ipGeneral router filter for information about this filter

ipTunnel

Description	IP tunnel
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Unexpected but recoverable events
Notice Log	No more pool space for interface up notification
Info	None
Debug	Function trace
Filter	None

ipv6AccessList

Description	IPv6 access list matching
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Access list rule has been matched
Debug	None
Filter 1:	accessList <ul style="list-style-type: none"> ■ accessList—Logs a match on any access-list entry for all IPv6 access lists
Filter 2:	accessList router <i>virtualRouterName</i> access-list <i>accessListName</i> access-element-id <i>idNumber</i> <ul style="list-style-type: none"> ■ accessList—Logs a match on any access-list entry ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ access-list—Logs events for a specific access list ■ <i>accessListName</i> —Name of access list for which you want to log events ■ access-element-id—Logs events for a specific element ID ■ <i>idNumber</i>—Element ID number for which you want to log events; the element ID is automatically assigned for access-list rules that you explicitly create and is shown by issuing the show ipv6 access-list detail command

ipv6General

Description	IPv6 general
Emergency	None
Alert	None
Critical	None
Error	License-related errors (for example, attempting to configure IPv6 without configuring the license first); error in sending interface up or down events to IPv6
Warning Log	Primary IPv6 address on an interface is not found
Notice Log	None
Info	None
Debug	None

Filter 1: interface *interfaceType interfaceSpecifier*

- interface—Logs events for a specific interface
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName* [interface *interfaceType interfaceSpecifier*]

- router—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events
- interface—Logs events on a specific interface on the virtual router
- *interfaceType*—Type of interface for which you want to log events (for example, atm or fastEthernet)
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

ipv6Interface

Description	IPv6 interface
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Interface configuration errors; errors in pointing interface to another interface; interface LocalAddress-related errors
Notice Log	None
Info	None
Debug	Interface state transitions
Filter 1:	interface—See description of the ipv6General interface filter for information about this filter
Filter 2:	router—See description of the ipv6General router filter for information about this filter

ipv6ProfileMgr

Description	IPv6 Profile Manager
Emergency	None
Alert	None
Critical	None
Error	Failure to create or delete dynamic IPv6 interfaces
Warning Log	None
Notice Log	None
Info	None
Debug	Events related to dynamic IPv6 interface creation or deletion; assignment or unassignment of profiles to interfaces
Filter	None

ipv6RouteTable

Description	IPv6 routing table
Emergency	None
Alert	None
Critical	None
Error	Next-hop resolution-related problems; exceeding maximum route limit or warning threshold; route add and delete errors
Warning Log	Route limit-related warnings
Notice Log	Route limit-related messages
Info	None
Debug	Normal routing table updates; next-hop resolution for static routes; redistribution events; overload list processing; routing table session creation; route change notification events; route add/delete information; route cleanup events
Filter 1:	interface—See description of the ipv6General interface filter for information about this filter
Filter 2:	router—See description of the ipv6General router filter for information about this filter

ipv6Traffic

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

ipv6Types

Description	IPv6 general
Emergency	None
Alert	None
Critical	System out of memory error for allocating IPv6 addresses; IPv6 shutdown started in all virtual routers
Error	System low on memory; IPv6 address allocation may fail
Warning Log	None
Notice Log	None
Info	None
Debug	None
Filter	None

isisAdjChange

Description	IS-IS adjacency up or down
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Adjacency state change
Info	None
Debug	None

Filter 1: interface *interfaceType interfaceSpecifier*

- interface—Logs events for a specific interface
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName* [interface *interfaceType interfaceSpecifier*]

- router—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events
- interface—Logs events on a specific interface on the virtual router
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

isisAdjPackets

Description	IS-IS adjacency hello packets
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Error in sent IIH or received IIH
Notice Log	Sent or received IIH, DR election
Info	Authentication failed
Debug	Detailed information about IIH
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisBfdEvents

Description	IS-IS and BFD interaction and IS-IS session log
Emergency	None
Alert	None
Critical	None
Error	BFD to IS-IS interaction failure errors; out of memory errors
Warning Log	None
Notice Log	None
Info	BFD session state changes
Debug	None
Filter	Router and interface

isisChecksumErr

Description	IS-IS checksum errors
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	LSP checksum error
Notice Log	None
Info	None
Debug	None
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisGeneral

Description	IS-IS system notifications
Emergency	None
Alert	None
Critical	None
Error	Error in restoring NVS
Warning Log	Exceeding maximum IP addresses on interface or maximum sequence number
Notice Log	Error in redistributing routes; LAN circuit coming up; BGP converged; BGP not converged and IS-IS times out; transient black hole avoidance suppressed because graceful restart has been configured and is in progress
Info	None
Debug	Redistributed routes
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisHelloGeneral

Description	IS-IS system notifications
Emergency	None
Alert	None
Critical	None
Error	Memory failure and other fatal errors
Warning Log	Communication failure between IS-IS and IS-IS hello
Notice Log	None
Info	None
Debug	Timer expiration and other normal events
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisHelloPackets

Description	IS-IS hello packets
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Hello packets sent and received
Debug	Dumping hello packet in detail
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisIpv6Log

Description	IS-IS IPv6 events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	IS-IS IPv6 events
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisLdpEvents

Description	Displays information about the interactions between LDP and IS-IS in the course of LDP-IGP synchronization.
Emergency	None
Alert	None
Critical	None
Error	Failure to communicate with LDP and out of memory conditions
Warning Log	None
Notice Log	None
Info	None
Debug	LDP interactions
Filter	None

isisLocalUpdate

Description	IS-IS local LSP packets
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Sent local LSP
Info	None
Debug	None
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisMplsTeAdvertisements

Description	IS-IS MPLS traffic engineering advertisements
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Resource information changes
Filter	None

isisMplsTeEvents

Description	IS-IS MPLS traffic engineering
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Start or stop MPLS function; tunnel in use by IS-IS; explicit route computation
Debug	Detailed debugging information for MPLS function
Filter	None

isisNsfEvents

Description	Log events related to IS-IS non-stop forwarding procedure during system warm start
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Logs IS-IS NSF timer related events (for example, expiration and cancellation of timers [T1, T2, T3])
Debug	Restart-request transmit; restart-ack receive; SNP receive processing; LSP synchronization; LSP purging
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisProtocolErr

Description	IS-IS protocol errors
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	LSP protocol error
Notice Log	None
Info	None
Debug	None
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

isisSnpPackets

Description	IS-IS complete sequence numbers PDU (CSNP) and partial sequence numbers PDU (PSNP) packets
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Error in received CSNP or PSNP
Notice Log	Sent PSNP; received CSNP or PSNP packets; PSNP authentication failed
Info	Sent CSNP packets; CSNP authentication failed
Debug	LSP entries
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isisSpfEvents

Description	IS-IS Shortest Path First (SPF)
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Start or suspend SPF; updating routing table
Info	Add tent or path; process LSP
Debug	Add route
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

isisSpfStatistics

Description	IS-IS SPF timing and statistic data
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	SPF compute time
Info	None
Debug	None
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

isisSpfTriggers

Description	IS-IS SPF triggering
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	SPF trigger event
Info	None
Debug	None
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

isisUpdatePackets

Description	IS-IS LSP packets sent or received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Error in received LSP
Notice Log	Sent or received LSP
Info	Authentication failed; processed received LSP
Debug	Set or cleared SRM flags; building LSP
Filter 1:	interface—See description of the isisAdjChange interface filter for information about this filter
Filter 2:	router—See description of the isisAdjChange router filter for information about this filter

isVoice

Description	IS Voice application
Emergency	None
Alert	None
Critical	None
Error	NVS error; out of resources error; unexpected error
Warning Log	IP request failed
Notice Log	LSP used by IP circuit changes state (up, down, or modified); IP circuit requested, updated, or removed
Info	Voice gateway session established, terminated, or replaced
Debug	Management get, set, create, and remove
Filter	None

itm

Description	IPSec transport mode
Emergency	None
Alert	None
Critical	None
Error	IPSec transport protocol interaction failures; interface engine interaction failures; IPSec transport profile configuration errors; interface configuration errors
Warning Log	Recoverable IPSec transport interface–related configuration and operational error
Notice Log	IPSec transport interface state change
Info	IPSec transport interface interaction with IKE protocol; interface pool usage
Debug	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
Filter	None

I2cGeneral

Description	Layer 2 Control application general
Emergency	None
Alert	None
Critical	None
Error	Signal protocol failures, out of resources errors
Warning Log	Signal unexpected but recoverable socket conditions
Notice Log	None
Info	None
Debug	Neighbor, socket events
Filter	None

I2cKeepAlive

Description	Layer 2 Control adjacency packets
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Adjacency protocol packet processing
Filter	None

I2cPacket

Description	Layer 2 Control protocol packets
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Signal recoverable, unexpected packet processing failures
Notice Log	None
Info	None
Debug	Protocol packet exchange
Filter	None

I2tp

Description	Layer 2 Tunneling Protocol
Emergency	None
Alert	None
Critical	Nonrecoverable error
Error	Configuration error
Warning Log	Protocol error; insufficient resources
Notice Log	Status change; protocol warnings
Info	Protocol operational information
Debug	Detailed debugging information
Filter	None

I2tpDialoutGenerator

Description	L2TP dial-out
Emergency	None
Alert	None
Critical	None
Error	Internal software consistency errors; dial-out service denial because of insufficient resources; dial-out session failure
Warning Log	Dial-out NVS consistency errors; restrictions on maximum simultaneous dial-out components
Notice Log	None
Info	Dial-out resource pool expansion
Debug	None
Filter	None

I2tpDisconnectCause

Description	L2TP disconnect cause
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Disconnect error code information generated at LAC
Debug	None
Filter	None

I2tpIpLowerBinding

Description	Lower binding for L2TP and IP
Emergency	None
Alert	None
Critical	None
Error	Virtual router does not have a configured router ID; virtual router has a null router ID
Warning Log	None
Notice Log	None
Info	None
Debug	None
Filter	None

I2tpStateMachine

Description	Layer 2 Tunnel Protocol state machine trace
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	State machine trace
Filter	None

IdpConnect

Description	LDP connection information
Emergency	None
Alert	None
Critical	None
Error	Memory allocation failure.
Warning Log	None
Notice Log	LDP connection creation and deletion information
Info	None
Debug	None
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpGeneral

Description	Label Distribution Protocol general events
Emergency	None
Alert	None
Critical	None
Error	Memory allocation failures; protocol interaction failures
Warning Log	Message processing errors
Notice Log	Interface transition; adjacency transition
Info	Minor timer processing error
Debug	LDP finite state machine transactions; RouteTable interaction transaction; message processing transaction
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpGracefulRestart

Description	LDP graceful restart events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	LDP Neighbor Graceful Restart state changes
Info	LDP Graceful Restart timer operation
Debug	LDP Graceful Restart debug message
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpHelloMessages

Description	Label Distribution Protocol hello message event
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	LDP hello message processing errors
Notice Log	LDP hello message reception and transmission
Info	LDP hello message processing and transmission transaction
Debug	LDP hello message processing and transmission transaction details
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpHelloMgr

Description	Displays details about the task dedicated for sending LDP hellos, the LDP hello manager
Emergency	None
Alert	None
Critical	None
Error	Memory allocation failure
Warning Log	None
Notice Log	Hello transmission failure due to interface down
Info	None
Debug	Hello transmission debug information
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

ldpInterface

Description	LDP interface
Emergency	None
Alert	None
Critical	None
Error	Failure to enable LDP on the interface
Warning Log	None
Notice Log	Interface up and interface down events
Info	None
Debug	Event with detailed interface parameters for normal operation
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ interface—Logs events on a specific interface on the virtual router ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

IdpMessages

Description	Label Distribution Protocol session message events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Minor TCP transmission error
Info	LDP session message processing and transmission transaction
Debug	None
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpPeer

Description	LDP peer events
Emergency	None
Alert	None
Critical	None
Error	LDP neighbor authentication setting failure
Warning Log	None
Notice Log	LDP neighbor authentication transaction
Info	None
Debug	LDP peer maintenance transaction
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

ldpShimInterface

Description	LDP shim interface
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	None
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none">■ router—Logs events for a specific virtual router■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events■ interface—Logs events on a specific interface on the virtual router■ <i>interfaceType</i>—Type of interface for which you want to log events■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

IdpSocket

Description	Displays details about the socket that is used to exchange LDP session messages and keep alives
Emergency	None
Alert	None
Critical	None
Error	Memory allocation failure
Warning Log	Socket creation failure
Notice Log	Socket creation and deletion information
Info	None
Debug	Socket send and receive information
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpTimer

Description	Displays details about LDP timer events; when a timer expires or is scheduled
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Timer event information
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpVpls

Description	Displays details about LDP signaling for VPLS configurations
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	VPLS failure
Notice Log	VPLS up and down state information
Info	None
Debug	VPLS debug information
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

IdpWorker

Description	Displays details about the background LDP jobs (LDP worker events)
Emergency	None
Alert	None
Critical	None
Error	Memory allocation failure
Warning Log	Invalid PDU
Notice Log	Worker creation and deletion information
Info	TCP socket reset by peer
Debug	Worker running information
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

localAddressServerGeneral

Description	LAS general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Attempts to set a local pool group name; attempts to restore an overlapping address range from a previous version of the software
Notice Log	None
Info	None
Debug	Control flow and key events
Filter	None

localAuthServer

Description	Local authentication server
Emergency	None
Alert	None
Critical	None
Error	Cannot bind to local authentication server; memory cannot be allocated for local authentication server; cannot send configuration request; cannot send information request; invalid virtual router; error with specified user database; cannot create local user database at startup
Warning Log	Internal AAA user profile missing; cannot create users at startup; user associated with invalid virtual router; users reassigned to default user database; invalid user database; cannot associate users with virtual router
Notice Log	None
Info	None
Debug	Server started; server bind occurred; no user name provided; no CHAP challenge provided; no authenticate request message allocated
Filter	None

localEnableAuthServer

Description	Authentication server using locally stored enable secret
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Connection granted: no secrets are configured
Notice Log	None
Info	None
Debug	Authentication attempted; no memory for protocol message; connection granted: correct password; connection denied: incorrect password
Filter	None

localLinePassword

Description	Local line password authentication server
Emergency	None
Alert	None
Critical	None
Error	Unknown algorithm for local password
Warning Log	Connection granted or denied due to possible misconfiguration
Notice Log	None
Info	None
Debug	Connection granted or denied due to incorrect password
Filter	None

macroData

Description	Macro information
Emergency	None
Alert	None
Critical	None
Error	Error while running the macro
Warning Log	None
Notice Log	Data from env.setResults
Info	None
Debug	None

mgmtGeneral

Description	IP multicast group table manager general information
Emergency	None
Alert	None
Critical	None
Error	Major errors in MGMT API calls resulting in failure
Warning Log	IP Multicast fastpath forwarding not supported on interface
Notice Log	Errors in MGMT API calls
Info	State change events; invalid parameters in API calls
Debug	(Source, Group) entries not found
Filter 1:	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> ■ interface—Logs events for a specific interface ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName* [interface *interfaceType* *interfaceSpecifier*]

- router—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events
- interface—Logs events on a specific interface on the virtual router
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

mgmtGracefulRestart

Description	MGTM graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Multicast graceful restart complete
Info	None
Debug	IGMP, PIM, IP route table multicast graceful restart complete
Filter	None

mgtmv6General

Description	IPv6 multicast group table manager general information
Emergency	None
Alert	None
Critical	None
Error	Major errors in MGTM API calls resulting in failure
Warning Log	IPv6 Multicast fastpath forwarding not supported on interface
Notice Log	Errors in MGTM API calls
Info	State change events; invalid parameters in API calls
Debug	(Source, Group) entries not found

Filter 1: interface *interfaceType interfaceSpecifier*

- interface—Logs events for a specific interface
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName* [interface *interfaceType interfaceSpecifier*]

- router—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events
- interface—Logs events on a specific interface on the virtual router
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

mgtmv6GracefulRestart

Description	MGTM V6 graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Multicast graceful restart complete
Info	None
Debug	IGMP, PIM, IP route table multicast graceful restart complete
Filter	None

mldGeneral

Description	Multicast Listener Discovery (MLD) general
Emergency	None
Alert	None
Critical	None
Error	Nonrecoverable errors
Warning Log	NVS errors
Notice Log	Errors while configuring or learning groups
Info	None

Debug MLD interface or group state change

Filter 1: interface *interfaceType interfaceSpecifier*

- interface—Logs events for a specific interface
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName* [interface *interfaceType interfaceSpecifier*]

- router—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events
- interface—Logs events on a specific interface on the virtual router
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

mldGracefulRestart

Description	MLD graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	IGMP/MLD graceful restart complete
Info	None
Debug	None
Filter	None

mldGroupState

Description	Multicast Listener Discovery (MLD) group state change events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	MLDv1 first host join, last host done events; MLDv2 state change and source-list change events aggregated across all hosts on the interface
Debug	None
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events ■ interface—Logs events on a specific interface on the virtual router ■ <i>interfaceType</i>—The type of the interface for which you want to log events. For example, atm or fastEthernet. ■ <i>interfaceSpecifier</i>—The location of the interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

mmcd

Description	MMC switch fabric driver
Emergency	None
Alert	None
Critical	None
Error	Errors in hardware configuration; resource limitation in fabric reached; errors in hardware
Warning Log	None
Notice Log	None
Info	None
Debug	Initialization details; configuration details; connection status details
Filter	None

mobileipv4HaBinding

Description	Mobile IPv4 home agent binding
Emergency	None
Alert	None
Critical	None
Error	Registration request (RRQ) from foreign agent is prohibited by host access control list (ACL)
Warning Log	None
Notice Log	None
Info	None
Debug	Mobile IP timer started for n seconds, where n is the number of seconds
Filter	None

mobileIpv4HaEng

Description	Mobile IPv4 home agent engineering
Emergency	None
Alert	None
Critical	None
Error	Home agent does not exist in the virtual router
Warning Log	None
Notice Log	Mobile IP warm restart initiated
Info	None
Debug	Verifying replay attack
Filter	None

mobileIpv4HaEvent

Description	Mobile IPv4 home agent events
Emergency	None
Alert	None
Critical	None
Error	Authentication check failed
Warning Log	None
Notice Log	None
Info	None
Debug	Authentication check succeeded
Filter	None

mobileIpv4HaLog

Description	Mobile IPv4 home agent log
Emergency	None
Alert	None
Critical	None
Error	Registration request sanity check failed
Warning Log	None
Notice Log	Home agent deactivated in virtual router
Info	Home agent activated in virtual router
Debug	Authentication, authorization, and accounting (AAA) granted
Filter	None

mplsFwdTable

Description	MPLS forwarding table events
Emergency	None
Alert	None
Critical	None
Error	Nonfatal internal errors
Warning Log	Minor nonfatal internal errors
Notice Log	None
Info	None
Debug	Addition, deletion, and modification of table entries
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

mplsGeneral

Description	MPLS general purpose
Emergency	None
Alert	None
Critical	None
Error	Nonfatal internal errors; configuration errors
Warning Log	Major interface deletion; minor internal errors
Notice Log	None
Info	NVS operations
Debug	NVS operations; timer operations; minor interface label stacking; function flows; L2VPN instance created, destroyed
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

mplsHighAvailability

Description	MPLS high availability events
Emergency	None
Alert	None
Critical	None
Error	Nonfatal internal errors
Warning Log	Minor nonfatal internal errors
Notice Log	None
Info	Recovery of state information from NVS and mirrored storage; high-availability interactions with MPLS signaling protocols and line cards (major events)
Debug	High-availability interactions with MPLS signaling protocols and line modules (minor events)
Filter	None

mplsMajorInterface

Description	MPLS major interface
Emergency	None
Alert	None
Critical	None
Error	Signaling protocol interaction failures; major interface engine interaction failures; major interface finite state machine bad state transitions; major interface configuration errors; LSM interface label space interaction failures
Warning Log	None
Notice Log	None
Info	None
Debug	Major interface finite state machine transitions; signaling protocol interaction; major interface to engine transactions; major interface configuration transactions; LSM interface label space transactions
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ interface—Logs events on a specific interface on the virtual router ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

mplsMinorInterface

Description MPLS minor interface

Emergency None

Alert None

Critical None

Error Tunnel/LSP setup or teardown signaling protocol interaction failures; minor interface engine interaction failures; minor interface finite state machine bad state transitions; minor interface configuration errors; minor interface to IP interaction failures

Warning Log None

Notice Log None

Info None

Debug Minor interface to engine transactions; minor interface to IP transactions; minor interface configuration transactions; signaling protocol LSP setup or teardown transactions; minor interface finite state machine transitions

Filter 1: interface *interfaceType interfaceSpecifier*

- interface—Logs events for a specific interface
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName*

- router—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events

mplsRouter

Description	MPLS router events
Emergency	None
Alert	None
Critical	None
Error	Nonfatal internal errors
Warning Log	Minor nonfatal internal errors
Notice Log	None
Info	Creation or removal of MPLS router
Debug	Configuration changes for per-VR attributes; dynamic interface creation events
Filter	None

mplsShimInterface

Description	MPLS Shim Interface events
Emergency	None
Alert	None
Critical	None
Error	Signaling protocol interaction failures; shim interface engine interaction failures; shim interface finite state machine bad state transitions; shim interface configuration errors
Warning Log	None
Notice Log	None
Info	None
Debug	Shim interface finite state machine transitions; signaling protocol interaction; shim interface to engine transactions; shim interface configuration transactions
Filter	<p>router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>]</p> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events ■ interface—Logs events on a specific interface on the virtual router ■ <i>interfaceType</i>—Type of the interface for which you want to log events. For example, atm. ■ <i>interfaceSpecifier</i>—Location of the interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

mplsTraffic

Description	Logging for MPLS slow-path, ping, and trace packets; MPLS packets exceptioned to the SRP module for any reason
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	MPLS packets discarded on transmit or receive for any reason
Notice Log	None
Info	Abnormal conditions encountered during MPLS packet processing (when packets are not discarded); for example, truncating a packet or ignoring packet fields
Debug	Detailed debugging information for all MPLS packets transmitted to and received from the SRP module
Filter	None

mrInfoLog

Description	General multicast router information
Emergency	None
Alert	None
Critical	None
Error	Application startup or shutdown failures, resource allocation failures
Warning Log	None
Notice Log	Protocol Errors on received packets
Info	None
Debug	Trace application startup/shutdown/operation
Filter	None

mrInfoRcvdLog

Description	Multicast router received information
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Number of trace packets received
Debug	Hexidecimal dump of packets received
Filter	None

mrInfoSentLog

Description	Multicast router sent information
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Number of trace packets sent
Debug	Hexidecimal dump of packets sent
Filter	None

mtraceLog

Description	General Mtrace server information
Emergency	None
Alert	None
Critical	None
Error	Error creating or deleting Mtrace server; error communicating with other modules; allocation failures
Warning Log	None
Notice Log	Error in received or sent mtrace packets
Info	None
Debug	Creation or deletion of Mtrace server; communication with other modules
Filter	None

mtraceRcvdLog

Description	mtrace packets received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the received mtrace packets
Debug	Complete print of the received mtrace packets
Filter	None

mtraceSentLog

Description	mtrace packets sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the mtrace packets sent
Debug	Complete print of the mtrace packets sent
Filter	None

multicastTraffic

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

nameResolverLog

Description	Name resolver table
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Name lookup failures
Debug	Name lookup processing events
Filter	None

nfsClient

Description	NFS client log
Emergency	None
Alert	None
Critical	None
Error	Error installing NFS driver; error mounting or unmounting remote file system with specific error indication (if known); error accessing file on remote file system
Warning Log	Attempting to reuse already used local mount point when mounting remote file system; attempting to unmount remote file system with outstanding open files
Notice Log	None
Info	NFS client driver installed or uninstalled; mounting or unmounting remote file system; opening or closing remote files
Debug	None
Filter	None

noneAaaAddrServer

Description	AAA address client
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Notification of automatic success response to address request
Filter	None

noneAaaServer

Description	Authentication and accounting client
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Notification of automatic success response to authentication or accounting request
Filter	None

ntpGeneral

Description	Network Time Protocol (NTP) system notifications
Emergency	None
Alert	None
Critical	None
Error	NVS configuration errors; insufficient memory resources; protocol errors; time adjustment failures
Warning Log	No usable servers, NTP synchronization lost
Notice Log	System time adjustment
Info	Attach to or detach from virtual router; shutting down NTP IP session; shutting down NTP UDP session; enable or disable NTP; connection established with NTP server; announce system clock precision
Debug	None
Filter	router ID

OS

Description	Operating system (including image loader)
Emergency	None
Alert	Fatal software error notification (assertions, panics, exceptions); panic timer expiration; ECC memory errors
Critical	System halt; NVS reverting to factory defaults
Error	File system errors; image checksum failure; POST test failure; unexpected software error; scheduled reload cancelled due to ongoing NVS flush; image not found or invalid; core dump host connect failure; SRP synchronization failure notification; I/O module mismatch or missing; NVS configuration errors
Warning Log	OsTask client failed to initialize; file system capacity low (15%); heap utilization high (85%); crash dump save failure; unknown reset type; image loader failures (will retry); boot ROM programming failure; hardware upgrade necessary notification; NVS config file read or write errors; release file invalid
Notice Log	OsAppRegistrar client names; OsAppRegistrar state change; version display; last reset type; file system condition abatement; POST start or done; NVS config file initialized or converted; scheduled reload notification; heap utilization abatement (75%); file system release file copy notification; erasing boot ROM notification; core dump notification and status; NVS config boot status (factory defaults, running, file)
Info	Image loader request; image loader success; SC-srpIc mailbox client up; POST test passed; NVS config cache enable, disable, flush, or termination; release path notification
Debug	High-frequency debug messages (enabled with various build defines); cached file hit, miss, or close; image loader frame retry; NVS config cache flush status
Filter	None

ospfElectDr

Description	OSPF designated router (DR) election
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	DR election events
Info	None
Debug	None
Filter 1:	<p>interface-ip-address [ip-address <i>ipAddress</i> unnumbered <i>interfaceType</i> <i>interfaceSpecifier</i>]</p> <ul style="list-style-type: none"> ■ interface-ip-address—Logs events for a specific interface ■ ip-address—Specifies that you will identify the interface by entering an IP address ■ <i>ipAddress</i>—IP address of interface for which you want to log events ■ unnumbered—Specifies that the interface is unnumbered ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of the unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

- Filter 2:** router *virtualRouterName* [interface-ip-address [ip-address *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier*]]
- router—Logs events for a specific virtual router
 - *virtualRouterName*—Name of virtual router for which you want to log events
 - interface-ip-address—Logs events for a specific interface on the virtual router
 - ip-address—Specifies that you will identify the interface by entering an IP address
 - *ipAddress*—IP address of interface for which you want to log events

- `unnumbered`—Specifies that the interface is unnumbered
- `interfaceType`—Type of interface for which you want to log events
- `interfaceSpecifier`—Location of the unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

ospfGeneral

Description	OSPF general
Emergency	None
Alert	None
Critical	None
Error	Error enabling or disabling OSPF; allocation errors
Warning Log	State change errors (for example, OSPF could not be enabled); errors creating or destroying an area, an OSPF range, or a virtual link; error enabling OSPF protocol
Notice Log	OSPF enabled or disabled; BFD enabled or disable on an OSPF interface
Info	Event for a dynamic neighbor
Debug	Bouncing adjacency with a neighbor
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfHelloPktsRcvd

Description	Processing of hello messages received on OSPF-enabled interfaces
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Invalid packet, hello parameters mismatch (area, network, hello and dead intervals, version, md5 digest)
Notice Log	None
Info	None
Debug	Received hello information (ip source/destination, length)
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events ■ interface—Logs events on a specific OSPF-enabled interface on the virtual router ■ <i>interfaceType</i>—Type of the interface for which you want to log events (for example, atm or fastEthernet) ■ <i>interfaceSpecifier</i>—Location of the interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

ospfHelloPktsSent

Description	Sending of hello messages on OSPF-enabled interfaces
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Information about hello messages sent on OSPF-enabled interfaces (ip source/destination, length)
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events ■ interface—Logs events on a specific OSPF-enabled interface on the virtual router ■ <i>interfaceType</i>—Type of the interface for which you want to log events (for example, atm or fastEthernet) ■ <i>interfaceSpecifier</i>—Location of the interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

ospfInterface

Description	OSPF interface
Emergency	None
Alert	None
Critical	None
Error	Error saving or restoring OSPF interface configuration
Warning Log	Errors for packets sent or received over the OSPF interface
Notice Log	Creation or deletion of OSPF interfaces
Info	None
Debug	None
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfLdpEvents

Description	Displays information about the interactions between LDP and OSPF in the course of LDP-IGP synchronization.
Emergency	None
Alert	None
Critical	None
Error	Failure to communicate with LDP and out of memory conditions
Warning Log	None
Notice Log	None
Info	None
Debug	LDP interactions
Filter	None

ospfLsa

Description	OSPF link-state advertisement (LSA) events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	LSA discard errors
Notice Log	LSA add, update, or delete events; LSA purge, refresh, and max-age events; LSA send and receive events (Ack, delayed Ack, retransmit)
Info	None
Debug	None
Filter 1:	neighbor <i>neighborIpAddress</i> <ul style="list-style-type: none"> ■ neighbor—Logs events associated with a specific neighbor ■ <i>neighborIpAddress</i>—IP address of neighbor for which you want to log events
Filter 2:	router <i>virtualRouterName</i> [neighbor <i>neighborIpAddress</i>] <ul style="list-style-type: none"> ■ router—Logs events on a specific virtual router ■ <i>virtualRouterName</i>—Virtual router on which you want to log events ■ neighbor—Logs events associated with a specific neighbor ■ <i>neighborIpAddress</i>—IP address of neighbor for which you want to log events

ospfNeighbor

Description	OSPF neighbor change
Emergency	None
Alert	None
Critical	None
Error	Neighbor MTU negotiation rejects
Warning Log	Flooding event errors; neighbor transition from Full state to Down state; invalid neighbor LSA requests; neighbor MTU negotiation mismatches
Notice Log	Database description neighbor exchange; neighbor state changes; neighbor retransmissions
Info	None
Debug	None
Filter 1:	neighbor—See description of the ospfLsa neighbor filter for information about this filter
Filter 2:	router—See description of the ospfLsa router filter for information about this filter

ospfPktsRcvd

Description	OSPF packet received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Packets discarded; validation errors
Notice Log	Number of LSAs packed in different packet types (LSA Ack, LSA update); packets received over Down interface
Info	None
Debug	Packets received description
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfPktsSent

Description	OSPF packet sent
Emergency	None
Alert	None
Critical	None
Error	Packet sent errors (for example, dropped OSPF packets)
Warning Log	None
Notice Log	Number of LSAs packed in different packet types (LSA Ack, LSA update)
Info	None
Debug	Packets sent description
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfRestart

Description	OSPF graceful restart events
Emergency	None
Alert	None
Critical	None
Error	Unexpected events during restart
Warning Log	None
Notice Log	None
Info	General information about significant restart operation events (for example, restart entry, exit, abort, and neighbor acquisition)
Debug	Details about restart operation events
Filter	router—See description of the ospfElectDr router filter for information about this filter

ospfRoute

Description	OSPF route
Emergency	None
Alert	None
Critical	None
Error	OSPF route addition, deletion, or replacement errors in the routing table
Warning Log	Errors for routes imported into OSPF
Notice Log	Forwarding address decision algorithm events
Info	OSPF route added to, replaced, or deleted from the routing table; route imported into OSPF
Debug	None
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfSpfExt

Description	OSPF SPF external calculation
Emergency	None
Alert	None
Critical	None
Error	Errors in adding, modifying, or removing entries in tentative path entry table (TENT) and path entry table (PATH)
Warning Log	None
Notice Log	SPF (Dijkstra Shortest Path First algorithm) chunking events (for example, number of LSAs processed in an SPF chunk)
Info	SPF results
Debug	Events in building TENT and PATH
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfSpfInter

Description	OSPF SPF interarea calculation
Emergency	None
Alert	None
Critical	None
Error	Errors in adding, modifying, or removing entries in tentative path entry table (TENT) and path entry table (PATH)
Warning Log	None
Notice Log	SPF chunking events (for example, number of LSAs processed in an SPF chunk)
Info	SPF results
Debug	Events in building TENT and PATH
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfSpfIntra

Description	OSPF SPF intra-area calculation
Emergency	None
Alert	None
Critical	None
Error	Errors in adding, modifying, or removing entries in tentative path entry table (TENT) and path entry table (PATH)
Warning Log	None
Notice Log	SPF chunking events (for example, number of LSAs processed in an SPF chunk)
Info	SPF results
Debug	Events in building TENT and PATH
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfTeDatabase

Description	OSPF traffic engineering database
Emergency	None
Alert	None
Critical	None
Error	Error in adding, deleting, or updating a record in the TE database
Warning Log	None
Notice Log	None
Info	General information about a record being added, deleted, or updated in the TE database
Debug	None
Filter	router name <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router name—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

ospfTeSpf

Description	OSPF traffic engineering SPF
Emergency	None
Alert	None
Critical	None
Error	Any error in constrained SPF calculation
Warning Log	None
Notice Log	information about explicit path found as a result of TE SPF; information about type of failure in finding a constrained path
Info	None
Debug	None
Filter	router name <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router name—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

ospfv3ElectDr

Description	OSPFv3 designated router (DR) election
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	DR election events
Info	None
Debug	None
Filter 1:	interface-ip-address [ip-address <i>ipAddress</i> unnumbered <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ interface-ip-address—Logs events for a specific interface ■ ip-address—Specifies that you will identify the interface by entering an IP address ■ <i>ipAddress</i>—IP address of interface for which you want to log events ■ unnumbered—Specifies that the interface is unnumbered ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of the unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

- Filter 2:** router *virtualRouterName* [interface-ip-address [ip-address *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier*]]
- router—Logs events for a specific virtual router
 - *virtualRouterName*—Name of virtual router for which you want to log events
 - interface-ip-address—Logs events for a specific interface on the virtual router
 - ip-address—Specifies that you will identify the interface by entering an IP address
 - *ipAddress*—IP address of interface for which you want to log events

- `unnumbered`—Specifies that the interface is unnumbered
- `interfaceType`—Type of interface for which you want to log events
- `interfaceSpecifier`—Location of the unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

ospfv3General

Description	OSPFv3 general
Emergency	None
Alert	None
Critical	None
Error	Error enabling or disabling OSPFv3; allocation errors
Warning Log	State change errors (for example, OSPFv3 could not be enabled); errors creating or destroying an area, an OSPFv3 range, or a virtual link
Notice Log	OSPFv3 enabled or disabled; BFD enabled or disable on an OSPF interface
Info	None
Debug	None
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfv3HelloPktsRcvd

Description	Processing of hello messages received on OSPFv3-enabled interfaces
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Invalid packet, hello parameters mismatch (area, network, hello and dead intervals, version, md5 digest)
Notice Log	None
Info	None
Debug	Received hello information (ip source/destination, length)
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events ■ interface—Logs events on a specific OSPFv3-enabled interface on the virtual router ■ <i>interfaceType</i>—Type of the interface for which you want to log events (for example, atm or fastEthernet) ■ <i>interfaceSpecifier</i>—Location of the interface in the appropriate format

ospfv3HelloPktsSent

Description	Sending of hello messages on OSPFv3-enabled interfaces
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Information about hello messages sent on OSPFv3-enabled interfaces (ip source/destination, length)
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events ■ interface—Logs events on a specific OSPFv3-enabled interface on the virtual router ■ <i>interfaceType</i>—Type of the interface for which you want to log events (for example, atm or fastEthernet) ■ <i>interfaceSpecifier</i>—Location of the interface in the appropriate format

ospfv3Interface

Description	OSPFv3 interface
Emergency	None
Alert	None
Critical	None
Error	Error saving or restoring OSPFv3 interface configuration
Warning Log	Errors for packets sent or received over the OSPFv3 interface
Notice Log	Creation or deletion of OSPFv3 interfaces
Info	None
Debug	None
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfV3Lsa

Description	OSPFv3 link-state advertisement (LSA) events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	LSA discard errors
Notice Log	LSA add, update, or delete events; LSA purge, refresh, and max-age events; LSA send and receive events (Ack, delayed Ack, retransmit)
Info	None
Debug	None
Filter 1:	neighbor <i>neighborIpAddress</i> <ul style="list-style-type: none"> ■ neighbor—Logs events associated with a specific neighbor ■ <i>neighborIpAddress</i>—IP address of neighbor for which you want to log events
Filter 2:	router <i>virtualRouterName</i> [neighbor <i>neighborIpAddress</i>] <ul style="list-style-type: none"> ■ router—Logs events on a specific virtual router ■ <i>virtualRouterName</i>—Virtual router on which you want to log events ■ neighbor—Logs events associated with a specific neighbor ■ <i>neighborIpAddress</i>—IP address of neighbor for which you want to log events

ospfv3Neighbor

Description	OSPFv3 neighbor change
Emergency	None
Alert	None
Critical	None
Error	Neighbor MTU negotiation rejects
Warning Log	Flooding event errors; neighbor transition from Full state to Down state; invalid neighbor LSA requests; neighbor MTU negotiation mismatches; disregarding graceful restart notification (when graceful restart helper mode is not configured and the router gets a Grace LSA from a neighbor); aborting graceful restart due to time out (when the Grace LSA expires before the neighbor exited graceful restart); aborting graceful restart help due to topology change
Notice Log	Database description neighbor exchange; neighbor state changes; neighbor retransmissions
Info	None
Debug	Router exits graceful restart; helping router with graceful restart
Filter 1:	neighbor—See description of the ospfLsa neighbor filter for information about this filter
Filter 2:	router—See description of the ospfLsa router filter for information about this filter

ospfv3PktsRcvd

Description	OSPFv3 packet received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Packets discarded; validation errors
Notice Log	Number of LSAs packed in different packet types (LSA Ack, LSA update); packets received over Down interface
Info	None
Debug	Packets received description
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfv3PktsSent

Description	OSPFv3 packet sent
Emergency	None
Alert	None
Critical	None
Error	Packet sent errors (for example, dropped OSPF packets)
Warning Log	None
Notice Log	Number of LSAs packed in different packet types (LSA Ack, LSA update)
Info	None
Debug	Packets sent description
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfv3Route

Description	OSPF route
Emergency	None
Alert	None
Critical	None
Error	OSPF route addition, deletion, or replacement errors in the routing table
Warning Log	Errors for routes imported into OSPF
Notice Log	Forwarding address decision algorithm events
Info	OSPF route added to, replaced, or deleted from the routing table; route imported into OSPF
Debug	None
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfV3SpfExt

Description	OSPFv3 SPF external calculation
Emergency	None
Alert	None
Critical	None
Error	Errors in adding, modifying, or removing entries in tentative path entry table (TENT) and path entry table (PATH)
Warning Log	None
Notice Log	SPF (Dijkstra Shortest Path First algorithm) chunking events (for example, number of LSAs processed in an SPF chunk)
Info	SPF results
Debug	Events in building TENT and PATH
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfV3SpfInter

Description	OSPFv3 SPF interarea calculation
Emergency	None
Alert	None
Critical	None
Error	Errors in adding, modifying, or removing entries in tentative path entry table (TENT) and path entry table (PATH)
Warning Log	None
Notice Log	SPF chunking events (for example, number of LSAs processed in an SPF chunk)
Info	SPF results
Debug	Events in building TENT and PATH
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

ospfV3SpfIntra

Description	OSPFv3 SPF intra-area calculation
Emergency	None
Alert	None
Critical	None
Error	Errors in adding, modifying, or removing entries in tentative path entry table (TENT) and path entry table (PATH)
Warning Log	None
Notice Log	SPF chunking events (for example, number of LSAs processed in an SPF chunk)
Info	SPF results
Debug	Events in building TENT and PATH
Filter 1:	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
Filter 2:	router—See description of the ospfElectDr router filter for information about this filter

pimAutoRPRcvdLog

Description	Protocol Independent Multicast (PIM) AutoRP messages received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of received PIM AutoRP packets
Debug	Complete print of received PIM AutoRP packets
Filter 1:	interface-ip-address [ip-address <i>ipAddress</i> unnumbered <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ interface-ip-address—Logs events for a specific interface ■ ip-address—Specifies that you will identify the interface by entering an IP address ■ <i>ipAddress</i>—IP address of interface for which you want to log events ■ unnumbered—Specifies that the interface is unnumbered ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2:	router <i>virtualRouterName</i> [interface-ip-address [ip-address <i>ipAddress</i> unnumbered <i>interfaceType</i> <i>interfaceSpecifier</i>]] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ interface-ip-address—Logs events for a specific interface on the virtual router ■ ip-address—Specifies that you will identify the interface by entering an IP address ■ <i>ipAddress</i>—IP address of interface for which you want to log events ■ unnumbered—Specifies that the interface is unnumbered
------------------	---

- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

pimAutoRPSentLog

Description	Protocol Independent Multicast (PIM) AutoRP messages sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the sent PIM AutoRP packets
Debug	Complete print of the sent PIM AutoRP packets
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimBsrRcvdLog

Description	Reception of PIM-SM IPv4 BSR messages (BSM and C-RP-Advs)
Emergency	None
Alert	None
Critical	None
Error	Parse errors
Warning Log	Context errors
Notice Log	None
Info	Description of received messages (specify high verbosity for detail)
Debug	None
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimBsrSentLog

Description	Transmission of PIM-SM IPv4 BSR messages (BSM and C-RP-Advs)
Emergency	None
Alert	None
Critical	None
Error	System errors
Warning Log	None
Notice Log	None
Info	Description of transmitted messages (specify high verbosity for detail)
Debug	None
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimGracefulRestartLog

Description	PIM graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	PIM graceful restart complete
Info	None
Debug	None
Filter	None

pimHelloRcvdLog

Description	Protocol Independent Multicast (PIM) hello messages received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the received PIM hello messages
Debug	Complete printout of the received PIM hello messages
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimHelloSentLog

Description	Protocol Independent Multicast (PIM) hello messages sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the PIM hello messages sent
Debug	Complete description of the PIM hello messages sent
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimIpv6AutoRPRcvdLog

Description	Protocol Independent Multicast (PIM) AutoRP messages received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of received PIM AutoRP packets
Debug	Complete print of received PIM AutoRP packets
Filter 1:	interface-ipv6-address [ipv6-address <i>ipv6Address</i> unnumbered <i>interfaceType interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ interface-ipv6-address—Logs events for a specific interface ■ ipv6-address—Specifies that you will identify the interface by entering an IPv6 address

- *ipv6Address*—IPv6 address of interface for which you want to log events
- *unnumbered*—Specifies that the interface is unnumbered
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: `router virtualRouterName [interface-ipv6-address [ipv6-address ipv6Address | unnumbered interfaceType interfaceSpecifier]]`

- *router*—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events
- *interface-ipv6-address*—Logs events for a specific interface on the virtual router
- *ipv6-address*—Specifies that you will identify the interface by entering an IPv6 address
- *ipv6Address*—IPv6 address of interface for which you want to log events
- *unnumbered*—Specifies that the interface is unnumbered
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

pimIpv6AutoRPSentLog

Description	Protocol Independent Multicast (PIM) AutoRP messages sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the sent PIM AutoRP packets
Debug	Complete print of the sent PIM AutoRP packets
Filter 1:	interface-ipv6-address—See description of the pimIpv6AutoRPRcvdLog interface-ipv6-address filter for information about this filter
Filter 2:	router—See description of the pimIpv6AutoRPRcvdLog router filter for information about this filter

pimIpv6BsrRcvdLog

Description	Reception of PIM-SM IPv6 BSR messages (BSM and C-RP-Advs)
Emergency	None
Alert	None
Critical	None
Error	Parse errors
Warning Log	Context errors
Notice Log	None
Info	Description of received messages (specify high verbosity for detail)
Debug	None
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimIpv6BsrSentLog

Description	Transmission of PIM-SM IPv6 BSR messages (BSM and C-RP-Advs)
Emergency	None
Alert	None
Critical	None
Error	System errors
Warning Log	None
Notice Log	None
Info	Description of transmitted messages (specify high verbosity for detail)
Debug	None
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimIpv6GracefulRestartLog

Description	PIM IPv6 graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	PIM graceful restart complete
Info	None
Debug	None
Filter	None

pimIpv6HelloRcvdLog

Description	Protocol Independent Multicast (PIM) hello messages received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the received PIM hello messages
Debug	Complete printout of the received PIM hello messages
Filter 1:	interface-ipv6-address [ipv6-address <i>ipv6Address</i> unnumbered <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ interface-ipv6-address—Logs events for a specific interface ■ ipv6-address—Specifies that you will identify the interface by entering an IPv6 address ■ <i>ipv6Address</i>—IPv6 address of interface for which you want to log events ■ unnumbered—Specifies that the interface is unnumbered ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2:	router <i>virtualRouterName</i> [interface-ipv6-address [ipv6-address <i>ipv6Address</i> unnumbered <i>interfaceType</i> <i>interfaceSpecifier</i>]] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ interface-ipv6-address—Logs events for a specific interface on the virtual router ■ ipv6-address—Specifies that you will identify the interface by entering an IPv6 address ■ <i>ipv6Address</i> —IPv6 address of interface for which you want to log events ■ unnumbered—Specifies that the interface is unnumbered
------------------	--

- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of unnumbered interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

pimIpv6HelloSentLog

Description	Protocol Independent Multicast (PIM) Hello messages sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the PIM hello messages sent
Debug	Complete description of the PIM hello messages sent
Filter 1:	interface-ipv6-address—See description of the pimIpv6HelloRcvdLog interface-ipv6-address filter for information about this filter
Filter 2:	router—See description of the pimIpv6HelloRcvdLog router filter for information about this filter

pimIpv6PktsRcvdLog

Description	Protocol Independent Multicast (PIM) nonhello (Register/RegisterStop/JoinPrune/Assert/Graft/GraftAck) messages received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the PIM messages received
Debug	Complete description of the PIM messages received
Filter 1:	interface-ipv6-address—See description of the pimIpv6HelloRcvdLog interface-ipv6-address filter for information about this filter
Filter 2:	router—See description of the pimIpv6HelloRcvdLog router filter for information about this filter

pimIpv6PktsSentLog

Description	Protocol Independent Multicast (PIM) nonhello (Register/RegisterStop/JoinPrune/Assert/Graft/GraftAck) messages sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the PIM messages sent
Debug	Complete description of the PIM messages sent
Filter 1:	interface-ipv6-address—See description of the pimIpv6HelloRcvdLog interface-ipv6-address filter for information about this filter
Filter 2:	router—See description of the pimIpv6HelloRcvdLog router filter for information about this filter

pimPktsRcvdLog

Description	Protocol Independent Multicast (PIM) nonhello (Register/RegisterStop/JoinPrune/Assert/Graft/GraftAck) messages received
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the PIM messages received
Debug	Complete description of the PIM messages received
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimPktsSentLog

Description	Protocol Independent Multicast (PIM) nonhello (Register/RegisterStop/JoinPrune/Assert/Graft/GraftAck) messages sent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Short description of the PIM messages sent
Debug	Complete description of the PIM messages sent
Filter 1:	interface-ip-address—See description of the pimAutoRPRcvdLog interface-ip-address filter for information about this filter
Filter 2:	router—See description of the pimAutoRPRcvdLog router filter for information about this filter

pimsmGeneral

Description	General PIM sparse mode events
Emergency	None
Alert	None
Critical	Failure to initialize PIM sparse mode; memory allocation failures
Error	Error enabling or disabling PIM sparse mode; error adding or removing state
Warning Log	None
Notice Log	None
Info	Successful addition or removal of peer
Debug	None
Filter	None

pimsmMvpn

Description	Multicast VPN events, including default and data MDT creation and deletion
Emergency	None
Alert	None
Critical	None
Error	Failure to create MDT
Warning Log	None
Notice Log	Successful creation or deletion of default MDT; switch from data MDT to default MDT or from default MDT to data MDT
Info	Successful creation or deletion of data MDT
Debug	None
Filter	None

policyMgrAttachment

Description	Policy Manager policy attachment activity
Emergency	None
Alert	None
Critical	None
Error	Error attaching policies to static and dynamic interfaces
Warning Log	None
Notice Log	None
Info	Successful attachment of policies to dynamic interfaces
Debug	None
Filter	None

policyMgrGeneral

Description	Policy Manager general information
Emergency	None
Alert	None
Critical	None
Error	Error storing or restoring policy manager data to and from NVS; resource exhaustion errors
Warning Log	None
Notice Log	None
Info	None
Debug	None
Filter	None

policyMgrPacketLog

Description	Policy Manager packets
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Packet trace
Debug	None
Filter	None

ppp

Description	Point-to-Point Protocol layer
Emergency	None
Alert	None
Critical	Nonrecoverable error
Error	Recoverable error
Warning Log	Resource or configuration problem
Notice Log	Authentication actions
Info	None
Debug	Detailed debugging information
Filter	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> ■ interface—Logs PPP events for a specific interface ■ <i>interfaceType</i>—Type of interface for which you want to log PPP events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

pppoe

Description	Point-to-Point over Ethernet layer
Emergency	None
Alert	None
Critical	None
Error	Error enabling control packet log
Warning Log	PPPoE interface or subInterface removed from NVS
Notice Log	PPPoE enabled; status change for subInterface
Info	Line module status change
Debug	None
Filter	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> ■ interface—Logs PPP events for a specific interface ■ <i>interfaceType</i>—Type of interface for which you want to log PPP events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

pppoeControlPacket

Description	PPPoE control packet trace
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Control packets logged; control packet log enabled
Filter	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none">■ <i>interface</i>—Logs PPP events for a specific interface■ <i>interfaceType</i>—Type of interface for which you want to log PPP events■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

pppPacket

Description	PPP packet capture
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Packet trace
Filter	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> ■ interface—Logs PPP events for a specific interface ■ <i>interfaceType</i>—Type of interface for which you want to log PPP events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

pppStateMachine

Description	PPP state machine trace
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	State machine trace
Filter	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none">■ <i>interface</i>—Logs PPP events for a specific interface■ <i>interfaceType</i>—Type of interface for which you want to log PPP events. For example, atm or fastEthernet■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

profileMgr

Description	Profile manager
Emergency	None
Alert	None
Critical	None
Error	Profile manager process creation failed
Warning Log	Profile being removed was not found
Notice Log	None
Info	None
Debug	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
Filter	None

qm

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

qos

Description	QoS events
Emergency	None
Alert	None
Critical	None
Error	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
Warning Log	None
Notice Log	None
Info	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
Debug	Dynamic attachment of QoS profile to interfaces
Filter	None

qosAttachment

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

radiusAttributes

Description	RADIUS user attributes
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Supported RADIUS attributes found in the Access-Accept or Access-Reject packet; reports changes to the Service-Acct-Interval attribute (Juniper VSA 26-140)
Filter	None

radiusClient

Description	RADIUS Authentication and Accounting Client
Emergency	None
Alert	None
Critical	None
Error	Internal allocation error of base RADIUS server table; invalid virtual router for user's context
Warning Log	Failure to send accounting on or accounting off; tunnel password format error; tunnel accounting request
Notice Log	Dropping tunnel attribute
Info	None
Debug	Authentication or accounting failure due to internal memory allocation failure
Filter	None

radiusCoAAttributes

Description	RADIUS CoA attributes
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Displays CoA requests and replies received by the router, including the attributes; reports changes to the Service-Acct-Interval attribute (Juniper VSA 26-140)
Filter	None

radiusDisconnectGeneral

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

radiusRelayGeneral

Description	RADIUS Relay Server general
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Memory-allocation; NVS update failure; subscriber session timeouts
Notice Log	None
Info	None
Debug	Receiving invalid radius request. Debugging interaction with AAA/GPLAAN
Filter	None

radiusSendAttributes

Description	RADIUS attributes added to outbound RADIUS requests
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Parse errors that occur in L2C and DSL Forum attribute strings
Debug	Attributes that are added to outbound RADIUS requests, including Access-Request, Acct-Start, Acct-Stop, interim accounting requests, and tunnel accounting requests
Filter	None

remOps

Description	Remote operations
Emergency	None
Alert	None
Critical	None
Error	Internal error
Warning Log	Maximum table size reached; ICMP failure; same target probed by more than one entry
Notice Log	Remote operations application begin/start; ping, traceroute, or nslookup entry; create, modify, or remove; unexpected packet receive; invalid target or source address; late packet receive
Info	None
Debug	Ping, traceroute, or nslookup session begin or end; packet receive; duplicate receive
Filter	None

resourceThresholdTrap

Description	Resource threshold trap log
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Rising trap
Notice Log	Falling trap
Info	None
Debug	None
Filter	None

ripBfd

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

ripGeneral

Description RIP system notifications

Emergency None

Alert None

Critical None

Error Failed to redistribute an external route to the RIP; failed to establish peer with neighbor due to the memory limitation; general RIP configuration error, such as an access list name or route map name specified in the RIP config mode exceed maximum allowable length

Warning Log Failed to process a RIP packet due to the current memory limitation

Notice Log Enable or disable RIP application

Info None

Debug RIP query; RIP peer address

Filter 1: interface *interfaceType interfaceSpecifier*

- interface—Logs PPP events for a specific interface
- *interfaceType*—Type of interface for which you want to log events
- *interfaceSpecifier*—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2: router *virtualRouterName*

- router—Logs events for a specific virtual router
- *virtualRouterName*—Name of virtual router for which you want to log events

ripRoute

Description	RIP route
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	None
Debug	Routes sent or received by RIP; if a route is rejected or not sent, gives the reason
Filter 1:	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> ■ interface—Logs PPP events for a specific interface ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

Filter 2:	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events
------------------	--

ripRtTable

Description	RIP routing table
Emergency	None
Alert	None
Critical	None
Error	Failed to remove a RIP route from the IP routing table
Warning Log	Failed to added a RIP route to the IP routing table
Notice Log	None
Info	None
Debug	Add or remove a route to the RIP routing table
Filter	None

routeDownloader

Description	RADIUS route-download server operation
Emergency	None
Alert	None
Critical	None
Error	Unable to create application process when configured
Warning Log	Write to mirrored storage memory failed
Notice Log	No IP Application is found on warm start; unable to retrieve a route from AAA; route string parse error; too many downloaded routes; invalid destination of a downloaded route; clear all command is terminated due to download failure; empty download
Info	Download started, completed, or finalized; IP update started, completed, or finalized
Debug	Download operation information; such as download request sent. download response received
Filter	None

routerLog

Description	Virtual router log
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Creation and deletion of virtual routers
Info	None
Debug	None
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

rsvpAsyncMgr

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

rsvpBfd

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

rsvpGeneral

Description	RSVP general purpose
Emergency	None
Alert	None
Critical	Initialization failures; fatal resource allocation failures; fatal internal errors.
Error	Signaling protocol errors; nonfatal internal errors; configuration errors
Warning Log	Minor internal errors
Notice Log	Very minor internal errors
Info	Minor internal errors
Debug	Function flows; parameter passing; timer operations
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

rsvpGracefulRestart

Description	RSVP graceful restart
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	RSVP graceful restart complete
Info	None
Debug	None
Filter	None

rsvpInterface

Description	RSVP interface
Emergency	None
Alert	None
Critical	None
Error	Setup errors; operational errors; invalid configuration errors
Warning Log	Nonfatal allocation errors
Notice Log	None
Info	Minor internal errors
Debug	Function flows
Filter	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ interface—Logs events on a specific interface on the virtual router ■ <i>interfaceType</i>—Type of interface for which you want to log events ■ <i>interfaceSpecifier</i>—Location of interface in the appropriate format



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

rsvpTunnel

Description	RSVP tunnels
Emergency	None
Alert	None
Critical	Critical operational errors
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 <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for traffic on a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router

security

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

serviceability

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

serviceMgr

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

serviceMgrClientSession

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

serviceMgrDcm

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

serviceMgrMacroManager

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

serviceMgrPerformance

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

serviceMgrServiceDef

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

serviceMgrServiceInstance

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

serviceMgrServiceSession

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

serviceMgrSubscriberSession

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

slep

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



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

snmp

Description	Embedded SNMP agent
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	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
Notice Log	None
Info	SNMP agent has been enabled or disabled
Debug	Trap request dropped; trap processing summary statistics
Filter	None

snmpIfMib

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

snmpPduAudit

Description	SNMP PDUs
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	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
Debug	None
Filter	None

snmpSetPduAudit

Description	SNMP set PDUs
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	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
Debug	None
Filter	None

snmpTrap

Description	SNMP Trap PDU events
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	SNMP trap PDUs that the corresponding SNMP agent transmitted
Debug	None
Filter	None

sonet

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

sonetPath

Description	SONET Path
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Errors during interface removal (for removable paths); path update failures from path configuration notification; failed mapping from SONET status; errors during path creation; engine addInterface errors during hwPresent notification; errors during path creation for nonchannelized interfaces; failed pool expansion
Notice Log	Pool expansion
Info	Init from NV failures; NV upgrade; path update progress; path configuration notification
Debug	Path update
Filter	None

sonetVT

Description	SONET virtual tributary
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Init from NV failures; errors during remove interface; failed pool expansion
Notice Log	Engine add interface retry; pool expansion
Info	Errors during add interface
Debug	None
Filter	None

ssccDetailPm

Description	SDX client (formerly SSCC) detail for policy manager (PM) interaction
Emergency	None
Alert	None
Critical	None
Error	Failure of policy manager calls (detail)
Warning Log	None
Notice Log	None
Info	None
Debug	Policy manager function call made; Policy manager attempts to get statistics
Filter	None

ssccDetailSsc

Description	SDX client (formerly SSCC) detail for SDX interaction
Emergency	None
Alert	None
Critical	None
Error	More detail for SDX management errors
Warning Log	None
Notice Log	None
Info	None
Debug	More detail for SDX events
Filter	None

ssccGeneral

Description	SDX client (formerly SSCC) general
Emergency	None
Alert	None
Critical	None
Error	Failure to get heap space; packet decode errors; SDX inconsistency errors; packet creation errors; failure of calls to policy manager (changing, attaching policy); attempt to manage unknown interface
Warning Log	None
Notice Log	None
Info	Creation or deletion of SDX client
Debug	Events (create interface, reports, removals); policy deletions; policy reattachments; CLI events; connection retries
Filter	None

ssh

Description	Secure Shell (SSH) Server
Emergency	None
Alert	None
Critical	None
Error	Cannot create SSH daemon; unexpected socket condition; packet overrun; AAA failure; resource allocation failure; host key read error
Warning Log	Missing/invalid public user key; possible DOS attack (invalid reported field length); unknown protocol message; protocol message received during wrong state; unsupported key exchange algorithm; unsupported cipher algorithm; unsupported encryption algorithm; unsupported MAC algorithm; unsupported compression algorithm; unexpected session/channel error; window adjust failure; user lock out announcement; user denied due to lock-out; packet encryption/decryption failure; unexpected protocol error; packet send failure; unsupported client version; malformed packet; packet MAC failure; user timeout
Notice Log	AAA user authentication failure; ignored channel request; client connect/disconnect
Info	Detailed client connection info (per connection attempt)
Debug	Daemon instance creation/removal; detailed packet info (per packet)
Filter	None

stTunnel

Description	Secure tunnel (ST) interface
Emergency	None
Alert	None
Critical	None
Error	ST interface configuration error; ST interface engine interaction failures; IPSec service line module resource error
Warning Log	ST interface pool exhausted; manual session key length input problems; problem relocating ST interface
Notice Log	ST interface memory pool extension
Info	Transport virtual router table downloading; ST interface status retrieval; transport virtual router table down; information about clear sa command
Debug	Detailed debug information related to the ST
Filter	None

stTunnelEngine

Description	Logs events and conditions related to the communication between the IPsec tunnels application and the IPsec server and line modules
Emergency	None
Alert	None
Critical	None
Error	Unexpected and nonrecoverable communication errors
Warning Log	Unexpected but recoverable events
Notice Log	Controller up/down and restart up/down events
Info	Processing of controller up/down and restart up/down events; processing of synchronization events following a cold- or warm-restart
Debug	Detailed debug information related to all communication between the IPsec tunnels application and the IPsec server and line modules; interactions with the IP Engine application for virtual router table download to designated IPsec server modules
Filter	None

system

Description	System management and monitoring
Emergency	None
Alert	None
Critical	Line module ping failure threshold exceeded
Error	Critical subsystem failure condition (NVS, power, fan, network timing, temperature); unrecognized module type; module ID mismatch; line module memory reduction; line module bandwidth misconfiguration; unrecoverable file system synchronization errors; software incompatibility issue
Warning Log	Noncritical subsystem failure condition (heap/CPU utilization, NVS, network timing); unexpected software error; recoverable file system synchronization errors; file system 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 <i>slotNumber</i> <ul style="list-style-type: none"> ■ slot—Logs events for a specific slot ■ <i>slotNumber</i>—Number of slot for which you want to log events

tacacsPlusServer

Description	TACACS + server
Emergency	None
Alert	None
Critical	None
Error	Unable to start TACACS + ; failed to create tacacsPlusProcess instance while in startup
Warning Log	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
Notice Log	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
Info	None
Debug	Authentication attempted while TACACS + is being shutdown; not enough memory for sending authentication requests; socket allocation limit reached; failed to allocate new socket for a request; not enough memory for protocol message; received unexpected notification on the socket
Filter	None

tcpGeneral

Description	TCP system
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	TCP state change event info (brief)
Info	None
Debug	TCP state changes (detail); TCP packet transmission; minor TCP errors
Filter	router <i>virtualRouterName</i> <ul style="list-style-type: none"> ■ router—Logs events for a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events

tcpTraffic

Description	TCP frame transmit and receive
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	TCP packet discards due to MD5 authorization failure and checksum failure
Info	None
Debug	Report all TCP receive and transmit events
Filter 1:	remote-ip-address <i>ipAddress</i> [<i>ipAddressMask</i>]
	<ul style="list-style-type: none"> ■ remote-ip-address—Logs events for a remote address ■ <i>ipAddress</i>—Address of remote system for which you want to log messages ■ <i>ipAddressMask</i>—Mask for the remote address
Filter 2:	router <i>virtualRouterName</i> [remote-ip-address <i>ipAddress</i> [<i>ipAddressMask</i>]]
	<ul style="list-style-type: none"> ■ router—Logs events on a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ remote-ip-address—Logs events for a remote address ■ <i>ipAddress</i>—Address of remote system for which you want to log messages ■ <i>ipAddressMask</i>—Mask for the remote address

tcpv6Traffic

Description	TCP frame transmit and receive
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	TCP packet discards due to MD5 authorization failure and checksum failure
Info	None
Debug	Report all TCP receive and transmit events
Filter 1:	remote-ip-address <i>ipAddress</i> [<i>ipAddressMask</i>]
	<ul style="list-style-type: none"> ■ remote-ip-address—Logs events for a remote address ■ <i>ipAddress</i>—Address of remote system for which you want to log messages ■ <i>ipAddressMask</i>—Mask for the remote address
Filter 2:	router <i>virtualRouterName</i> [remote-ip-address <i>ipAddress</i> [<i>ipAddressMask</i>]]
	<ul style="list-style-type: none"> ■ router—Logs events on a specific virtual router ■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events ■ remote-ip-address—Logs events for a remote address ■ <i>ipAddress</i>—Address of remote system for which you want to log messages ■ <i>ipAddressMask</i>—Mask for the remote address

telnet

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

telnetClient

Description	Telnet client log
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	Unexpected socket condition; unable to connect to remote host; successful connection; ENV send failure; resource allocation failure
Info	Connection attempt; detailed connection information (per connection); escape character announcement; connection closed
Debug	None
Filter	None

tftpClient

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

trackerEvents

Description	Tracker event propagation
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	None
Notice Log	None
Info	Indicates if there is a memory shortage for event propagation
Debug	Provides debug information for event propagation from the tracker component
Filter	None

trackerGeneral

Description	Tracker component
Emergency	None
Alert	None
Critical	None
Error	None
Warning Log	Indicates if there is a memory shortage for tracker operations
Notice Log	None
Info	Indicates if there is a memory shortage for accommodating new clients
Debug	Provides debug information for the tracker component
Filter	None

tsm

Description	Tunnel server manager
Emergency	None
Alert	None
Critical	Number of interfaces in use is critically close to maximum
Error	Memory exhaustion errors
Warning Log	Nonvolatile storage integrity problems; memory exhaustion-based denial of service; number of interfaces in use reaching high levels
Notice Log	Nonvolatile storage allocation problems; memory pool expansion
Info	Resource-restriction based denial of service; line module up or down transitions
Debug	Program debugging information including function call tracing
Filter	None

udpTraffic

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

udpv6Traffic

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

vrrp

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



NOTE: For information about interface types and specifiers, see *JUNOS Command Reference Guide, About This Guide*.

-
- *vrrpIdentifier*—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
Info	Replay of unknown interface after high availability switchover
Debug	General VSM operations, such as agent-circuit-id-based VLAN created
Filter	None

vsmEngine

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

Index

A

audience for documentation xiii

B

baseline commands
 baseline log 3

C

conventions defined
 icons xiv
 text and syntax xiv
customer support, contacting xx

D

destination
 logging messages by 4
documentation set, E-series and JUNOS xvi
 comments on xx
 obtaining xix

E

E120 routers xiv, xvi
E320 routers xiv, xvi
engineering logs
 enabling 6
ERX-14xx models xiv
ERX-310 router xiv
ERX-7xx models xiv
E-series and JUNOS documentation set xvi
 comments on xx
 obtaining xix
E-series router models xiv

F

fields
 adding to logs 6

I

icons defined, notice xiv

J

JUNOS software CD xviii

L

log commands
 baseline log 3
 log destination 4

log engineering 6
log field 6
log here 6
log severity 7
log unlimit 7
log verbosity 8
no log filters 15

See also show log commands

log event categories 21
 aaaAtm1483Cfg 21
 aaaEngineGeneral 22
 aaaQosCfg 22
 aaaServerGeneral 23
 aaaUserAccess 23
 addressServerGeneral 24
 ar1AaaServerGeneral 24
 atm 25
 atm1483 26
 atm1483VcClass 27
 atmAal5 27
 atmVcClass 28
 auditIpsec 28
 bfdAdaptivity 29
 bfdEvents 29
 bfdGeneral 30
 bfdSession 30
 bgpConnections 31
 bgpDampening 32
 bgpEvents 33
 bgpGeneral 34
 bgpGracefulRestart 35
 bgpIpv6NextHops 36
 bgpKeepAlives 37
 bgpMessages 38
 bgpNeighborChanges 39
 bgpNextHops 40
 bgpRoutes 41
 bridge 44
 bridgeEngine 44
 bridgingMgr 45
 bulkStats 45
 cacGeneral 46
 cacIntf 46
 cliCommand 47
 cliGeneral 47
 connectionManager 48
 cops 48
 copsPr 49
 coreDump 49

ctreeLog	50	ipEngine	87
dcm	50	ipflowstats	87
dcmEngineGeneral	51	ipflowstatsEngine	88
dhcpCapture	51	ipGeneral	88
dhcpExternal	52	ipIfCreator	89
dhcpExternalEngine	52	ipInterface	90
dhcpGeneral	53	ipNhopTrackerGeneral	90
dhcpIssuLog	53	ipProfileMgr	91
dhcpLocalClients	54	ipRoutePolicy	91
dhcpLocalGeneral	55	ipRouteTable	92
dhcpLocalHighAvailability	55	ipseclDb	92
dhcpLocalPool	56	ipsecP1 Throttler	93
dhcpLocalProtocol	57	ipsecXcfgSM	93
dhcpNvGeneral	58	ipSubscriberMgr	94
dhcpOfferLog	58	ipTraffic	94
dhcpPbeGeneral	59	ipTunnel	95
dhcpProxyGeneral	59	ipv6AccessList	96
dhcpRelayGeneral	60	ipv6General	97
dhcipv6Client	60	ipv6Interface	98
dhcipv6DemuxGeneral	61	ipv6ProfileMgr	98
dhcipv6LsGeneral	61	ipv6RouteTable	99
dismanEventMgr	62	ipv6Traffic	100
dnsGeneralLog	62	ipv6Types	101
DOSProtection	63	isisAdjChange	102
ds1	63	isisAdjPackets	103
ds3	64	isisBfdEvents	103
dvmrpGeneral	64	isisChecksumErr	104
dvmrpGracefulRestart	65	isisGeneral	104
dvmrpMcastTable	66	isisHelloGeneral	105
dvmrpProbeRcv	67	isisHelloPackets	105
dvmrpProbeSent	67	isisIpv6Log	106
dvmrpRtTable	68	isisLdpEvents	106
ethernet	68	isisLocalUpdate	107
ethernetStateSession	69	isisMplsTeAdvertisements	107
fileSystem	69	isisMplsTeEvents	108
flowInspection	70	isisNsfEvents	108
flowInspectionEngine	70	isisProtocolErr	109
flowServicesFirewallAlert	71	isisSnpPackets	109
flowServicesFirewallAudit	71	isisSpfEvents	110
frameRelay	72	isisSpfStatistics	110
fsAgent	72	isisSpfTriggers	111
ft1	73	isisUpdatePackets	111
ftpClient	73	isVoice	112
ftpServer	74	itm	112
gplaan	74	l2cGeneral	113
ha	75	l2cKeepAlive	113
hdlc	75	l2cPacket	114
hotfixGeneral	76	l2tp	114
httpServer	77	l2tpDialoutGenerator	115
icImageFixServer	78	l2tpDisconnectCause	115
icmpTraffic	79	l2tpLowerBinding	116
icmpv6Traffic	80	l2tpStateMachine	116
igmpGeneral	81	ldpConnect	117
igmpGracefulRestart	82	ldpGeneral	117
igmpGroupState	83	ldpGracefulRestart	118
ikeCertificateMgr	84	ldpHelloMessages	118
ikeEnrollment	84	ldpHelloMgr	119
ikepki	85	ldpInterface	120
interModuleCommunication	85	ldpMessages	121
ipAccessList	86	ldpPeer	121

ldpShimInterface	122	ospfv3ElectDr	162
ldpSocket	123	ospfv3General	163
ldpTimer	123	ospfv3HelloPktsRcvd	164
ldpVpls	124	ospfv3HelloPktsSent	165
ldpWorker	124	ospfv3Interface	166
localAddressServerGeneral	125	ospfv3Lsa	167
localAuthServer	125	ospfv3Neighbor	168
localEnableAuthServer	126	ospfv3PktsRcvd	169
localLinePassword	126	ospfv3PktsSent	169
macroData	127	ospfv3Route	170
mgmtGeneral	127	ospfv3SpfExt	170
mgmtGracefulRestart	128	ospfv3SpfInter	171
mgmtv6General	129	ospfv3SpfIntra	171
mgmtv6GracefulRestart	130	pimAutoRPRcvdLog	172
mldGeneral	131	pimAutoRPSentLog	173
mldGracefulRestart	132	pimBsrRcvdLog	174
mldGroupState	133	pimBsrSentLog	174
mmcd	134	pimGracefulRestartLog	175
mobileIpv4HaBinding	134	pimHelloRcvdLog	175
mobileIpv4HaEng	135	pimHelloSentLog	176
mobileIpv4HaEvent	135	pimIpv6AutoRPRcvdLog	176
mobileIpv4HaLog	136	pimIpv6AutoRPSentLog	178
mplsFwdTable	136	pimIpv6BsrRcvdLog	178
mplsGeneral	137	pimIpv6BsrSentLog	179
mplsHighAvailability	137	pimIpv6GracefulRestartLog	179
mplsMajorInterface	138	pimIpv6HelloRcvdLog	180
mplsMinorInterface	139	pimIpv6HelloSentLog	181
mplsRouter	140	pimIpv6PktsRcvdLog	182
mplsShimInterface	141	pimIpv6PktsSentLog	182
mplsTraffic	142	pimPktsRcvdLog	183
mrInfoLog	142	pimPktsSentLog	183
mrInfoRcvdLog	143	pimsmGeneral	184
mrInfoSentLog	143	pimsmMvpn	184
mtraceLog	144	policyMgrAttachment	185
mtraceRcvdLog	144	policyMgrGeneral	185
mtraceSentLog	145	policyMgrPacketLog	186
multicastTraffic	146	ppp	186
nameResolverLog	147	pppoe	187
nfsClient	147	pppoeControlPacket	188
noneAaaAddrServer	148	pppPacket	189
noneAaaServer	148	pppStateMachine	190
ntpGeneral	149	profileMgr	191
os	150	qm	191
ospfElectDr	151	qos	192
ospfGeneral	152	qosAttachment	192
ospfHelloPktsRcvd	153	radiusAttributes	193
ospfHelloPktsSent	154	radiusClient	193
ospfInterface	155	radiusCoAAttributes	194
ospfLdpEvents	155	radiusDisconnectGeneral	194
ospfLsa	156	radiusRelayGeneral	195
ospfNeighbor	157	radiusSendAttributes	195
ospfPktsRcvd	157	remOps	196
ospfPktsSent	158	resourceThresholdTrap	196
ospfRestart	158	ripBfd	197
ospfRoute	159	ripGeneral	198
ospfSpfExt	159	ripRoute	199
ospfSpfInter	160	ripRtTable	200
ospfSpfIntra	160	routeDownloader	200
ospfTeDatabase	161	routerLog	201
ospfTeSpf	161	rsvpAsyncMgr	201

rsvpBfd	202	N	
rsvpGeneral	202	notice icons defined	xiv
rsvpGracefulRestart	203	P	
rsvpInterface	204	platform considerations	
rsvpTunnel	205	system logs	2
security	205	R	
serviceability	206	release notes	xviii
serviceMgr	206	S	
serviceMgrClientSession	207	service commands	
serviceMgrDcm	207	service timestamps	13
serviceMgrMacroManager	208	show log commands	
serviceMgrPerformance	208	show log configuration	16
serviceMgrServiceDef	209	show log data	19
serviceMgrServiceInstance	209	software, installing or updating	xiii
serviceMgrServiceSession	210	support, requesting	xx
serviceMgrSubscriberSession	210	system event logs	
slep	211	individual logs	8, 12
snmp	211	severity	1
snmpIfMib	212	strategies	21
snmpPduAudit	212	system-wide logs	8, 12
snmpSetPduAudit	213	user-defined classification	14
snmpTrap	213	verbosity	2
sonet	214	viewing logs	19
sonetPath	214	T	
sonetVT	215	technical support, requesting	xx
ssccDetailPm	215	text and syntax conventions defined	xiv
ssccDetailSsc	216		
ssccGeneral	216		
ssh	217		
stTunnel	217		
stTunnelEngine	218		
system	219		
tacasPlusServer	220		
tcpGeneral	220		
tcpTraffic	221		
tcpv6Traffic	222		
telnet	223		
telnetClient	223		
tftpClient	224		
trackerEvents	224		
trackerGeneral	225		
tsm	225		
udpTraffic	226		
udpv6Traffic	227		
vrrp	228		
vrrpTracking	229		
vsm	229		
vsmEngine	230		
M			
manuals, E-series and JUNOS	xvi		
comments on	xx		
MIBs (Management Information Bases)	xix		
models			
E120	xiv		
E320	xiv		
ERX-14xx	xiv		
ERX-310	xiv		
ERX-7xx	xiv		