



**JUNOS<sup>™</sup>e Software  
for E-series<sup>™</sup> Routing Platforms**

**System Event Logging  
Reference Guide**

*Release 9.1.x*

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://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 9.1.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  
18 April 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](http://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

	<b>About This Guide</b>	<b>xiii</b>
	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
<b>Chapter 1</b>	<b>System Logging Overview</b>	<b>1</b>
	Overview of System Logging.....	1
	Log Severity .....	1
	Log Verbosity .....	2
	Persistent Logs .....	2
	Logging Platform Considerations.....	3
	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 Log Filters .....	15
	Monitoring Logging System Events .....	16
<b>Chapter 2</b>	<b>Event Categories</b>	<b>21</b>
	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
isisSnmpPackets .....	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<sup>e</sup>™ 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<sup>e</sup> 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<sup>e</sup> 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<sup>e</sup> System Basics Configuration Guide, Chapter 3, Installing JUNOS<sup>e</sup> Software*.



**NOTE:** If the information in the latest *JUNOS<sup>e</sup> Release Notes* differs from the information in this guide, follow the *JUNOS<sup>e</sup> 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
<b>Text Conventions</b>		
<b>Bold text like this</b>	Represents commands and keywords in text.	<ul style="list-style-type: none"> <li>■ Issue the <b>clock source</b> command.</li> <li>■ Specify the keyword <b>exp-msg</b>.</li> </ul>
<b>Bold text like this</b>	Represents text that the user must type.	host1(config)# <b>traffic class low-loss1</b>
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"> <li>■ Emphasizes words.</li> <li>■ Identifies variables.</li> <li>■ Identifies chapter, appendix, and book names.</li> </ul>	<ul style="list-style-type: none"> <li>■ There are two levels of access, <i>user</i> and <i>privileged</i>.</li> <li>■ <i>clusterId</i>, <i>ipAddress</i>.</li> <li>■ <i>Appendix A, System Specifications</i>.</li> </ul>
Plus sign ( + ) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<b>Syntax Conventions in the Command Reference Guide</b>		
Plain text like this	Represents keywords.	terminal length
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>
(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
<b>E-series Hardware Documentation</b>	
<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"> <li>■ Installing the chassis and modules</li> <li>■ Connecting cables</li> <li>■ Powering up the routers</li> <li>■ Configuring the routers for management access</li> <li>■ Troubleshooting common issues</li> </ul> <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"> <li>■ Installing the chassis and modules</li> <li>■ Connecting cables</li> <li>■ Powering up the routers</li> <li>■ Configuring the routers for management access</li> <li>■ Troubleshooting common issues</li> </ul> <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"> <li>■ ERX-7xx models</li> <li>■ ERX-14xx models</li> <li>■ ERX-310 router</li> </ul>
<b>JUNOS® Software Guides</b>	
<i>JUNOS® System Basics Configuration Guide</i>	Provides information about: <ul style="list-style-type: none"> <li>■ Planning and configuring your network</li> <li>■ Using the command-line interface (CLI)</li> <li>■ Installing JUNOS® software</li> <li>■ Configuring the Simple Network Management Protocol (SNMP)</li> <li>■ Managing the router and its modules, including the use of high availability (HA) for SRP redundancy</li> <li>■ Configuring and running a unified in-service software upgrade (ISSU)</li> <li>■ Configuring passwords and security</li> <li>■ Configuring the router clock</li> <li>■ Configuring virtual routers</li> </ul>
<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"> <li>■ Routing policies</li> <li>■ Firewalls</li> <li>■ Network Address Translation (NAT)</li> <li>■ J-Flow statistics</li> <li>■ Bidirectional forwarding detection (BFD)</li> <li>■ Internet Protocol Security (IPSec)</li> <li>■ Access Node Control Protocol (ANCP), also known as Layer 2 Control (L2C)</li> <li>■ Digital certificates</li> <li>■ IP tunnels</li> <li>■ Virtual Router Redundancy Protocol (VRRP)</li> <li>■ Mobile IP home agent</li> </ul>
<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"> <li>■ Internet Group Management Protocol (IGMP)</li> <li>■ Protocol Independent Multicast (PIM)</li> <li>■ Distance Vector Multicast Routing Protocol (DVMRP)</li> <li>■ Multicast Listener Discovery (MLD)</li> </ul>

**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"> <li>■ Border Gateway Protocol (BGP) routing</li> <li>■ Multiprotocol Label Switching (MPLS) and related applications</li> <li>■ Layer 2 services over MPLS</li> <li>■ Virtual private LAN service (VPLS)</li> <li>■ Layer 2 virtual private networks (L2VPNs)</li> </ul>
<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"> <li>■ Traffic classes and traffic-class groups</li> <li>■ Drop, queue, QoS, and scheduler profiles</li> <li>■ QoS parameters</li> <li>■ Statistics</li> </ul>
<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"> <li>■ Authentication, authorization, and accounting (AAA)</li> <li>■ Dynamic Host Configuration Protocol (DHCP)</li> <li>■ Remote Authentication Dial-In User Service (RADIUS)</li> <li>■ Terminal Access Controller Access Control System (TACACS+)</li> <li>■ Layer 2 Tunneling Protocol (L2TP)</li> <li>■ Subscriber management</li> </ul>
<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"> <li>■ Descriptions of commands and command parameters</li> <li>■ Command syntax</li> <li>■ A command's related mode</li> <li>■ Starting with JUNOS Release 7.1.0, a history of when a command, its keywords, and its variables were introduced or added</li> </ul> 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.
<b>Release Notes</b>	
<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<sup>e</sup> Configuration Guides**

JUNOS<sup>e</sup> 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<sup>e</sup> System Basics Configuration Guide, Chapter 1, Planning Your Network*.

The chapters in JUNOS<sup>e</sup> 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 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](mailto: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 of System Logging on page 1
- Logging Platform Considerations on page 3
- Configuring Event Logging on page 3
- Configuring Log Severity for Individual and Systemwide Logs on page 8
- Configuring Log Verbosity for Individual Logs or All Logs on page 12
- Setting the Timestamp for Log Messages on page 12
- Configuring Log Filters on page 14
- Turning Off Log Filters on page 15
- Monitoring Logging System Events on page 16

## Overview of System Logging

---

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

### Log Severity

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

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



## Logging 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.

5. 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.

6. 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.

7. 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 Log 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

---

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

## aaaEngineGeneral

---

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

## aaaQosCfg

---

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

## aaaServerGeneral

---

<b>Description</b>	AAA server general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Subscriber count exceeds license plus grace; internal attachment errors
<b>Warning Log</b>	Subscriber count exceeds license; cannot grow internal memory pools; accounting message failures
<b>Notice Log</b>	Authentication failures resulting from memory allocation failures
<b>Info</b>	None
<b>Debug</b>	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
<b>Filter</b>	None

## aaaUserAccess

---

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

## addressServerGeneral

---

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

## ar1AaaServerGeneral

---

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

**atm**


---

<b>Description</b>	ATM interface
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Unable to reenable ILMI administrative state after UNI version change
<b>Warning Log</b>	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
<b>Notice Log</b>	Interface pool expanded by an incremental number of entries; report retry delay in seconds when waiting for the underlying physical interface to be created; unable to allocate a message to send an interface up or down notification; unable to add or configure interface
<b>Info</b>	Dropping interface up, down, or not present notification due to removal of interface; discarding F4 OAM circuits when interface does not support F4 OAM
<b>Debug</b>	None
<b>Filter</b>	None

**atm1483**

---

**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**

---

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

**atmAal5**

---

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

**atmVcClass**

---

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

**auditIpsec**

---

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

## bfdAdaptivity

---

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

## bfdEvents

---

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

## bfdGeneral

---

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

## bfdSession

---

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

## bgpConnections

---

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

## bgpDampening

---

<b>Description</b>	BGP dampening
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	Route is suppressed by route-flap dampening; route is no longer suppressed by route-flap dampening
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter 1:</b>	access-class—This filter is not currently supported
<b>Filter 2:</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3:</b>	route-map—This filter is not currently supported
<b>Filter 4:</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5:</b>	in—This filter is not currently supported
<b>Filter 6:</b>	out—This filter is not currently supported

## bgpEvents

---

<b>Description</b>	BGP finite state machine (FSM) events and transitions
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Event occurred that was not expected for current state
<b>Warning Log</b>	None
<b>Notice Log</b>	One of the following events occurred: start, stop, inbound-connection-arrived, outbound-connection-complete, connection-error, connection-closed, start-timer-expired, connect-timer-expired, hold-timer-expired, keep-alive-timer-expired, open-received, update-received, keep-alive-received, notification-received, route-refresh, route-refresh-cisco
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter 1:</b>	access-class—This filter is not currently supported
<b>Filter 2:</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3:</b>	route-map—This filter is not currently supported
<b>Filter 4:</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5:</b>	in—This filter is not currently supported
<b>Filter 6:</b>	out—This filter is not currently supported

## bgpGeneral

---

<b>Description</b>	BGP general information
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	BGP IPv4 route-target-signaling address family enabled or disabled
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter 1:</b>	access-class—This filter is not currently supported
<b>Filter 2:</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3:</b>	route-map—This filter is not currently supported
<b>Filter 4:</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5:</b>	in—This filter is not currently supported
<b>Filter 6:</b>	out—This filter is not currently supported



## bgpGracefulRestart

---

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

## bgplpv6NextHops

---

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

## bgpKeepAlives

---

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



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

---

## bgpMessages

---

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

---

<b>Description</b>	BGP neighbor change
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	A peer has entered into or left the established state; reason for a session going idle
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter 1:</b>	access-class—This filter is not currently supported
<b>Filter 2:</b>	peer—See description of the bgpRoutes peer filter for information about this filter
<b>Filter 3:</b>	route-map—This filter is not currently supported
<b>Filter 4:</b>	router—See description of the bgpRoutes router filter for information about this filter
<b>Filter 5:</b>	in—This filter is not currently supported
<b>Filter 6:</b>	out—This filter is not currently supported

## bgpNextHops

---

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

## bgpRoutes

---

<b>Description</b>	BGP routing table updates
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Failure to add, remove, or modify BGP route in IP forwarding table
<b>Notice Log</b>	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
<b>Info</b>	None
<b>Debug</b>	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>
<b>Filter 1:</b>	<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"> <li>■ access-class—Logs events for traffic that matches a specific access class</li> <li>■ <i>accessClassName</i> —Name of the access class for which you want to log events</li> <li>■ route-map—Logs events for traffic that matches a specific route map</li> <li>■ <i>routeMapName</i>—Name of route map for which you want to log events</li> <li>■ <i>routeMapOptions</i>—In the following format—filtering-router <i>filteringRouterName</i> <i>filteringRouterOptions</i>   in   out</li> <li>■ filtering-router—Logs events only if the access class or route map are defined on a specific virtual router</li> <li>■ <i>filteringRouterName</i>—Virtual router where the access class or route map or both are defined</li> <li>■ <i>filteringRouterOptions</i>—in   out</li> </ul>

- 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**


---

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

**bridgeEngine**


---

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

**bridgingMgr**


---

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

**bulkStats**


---

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

**cacGeneral**


---

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

**cacIntf**


---

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



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

---

**cliCommand**


---

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

**cliGeneral**


---

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

## connectionManager

---

<b>Description</b>	Logging various conditions in the component that manages the chassis fabric.
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	10G and 5G SRP modules only—Detection that the FPGAs have not been loaded (results in an SRP [and chassis] reset)
<b>Error</b>	10G and 5G SRP modules only—That there is not enough bandwidth for a particular board in the system, that connections could not be added in the fabric due to resource limitations (such as memory), that a board was just removed and the resource will not be needed when this condition is detected momentarily, or that a connection cannot be closed or a multicast destination cannot be dropped.
<b>Warning Log</b>	Cannot connect to a particular source or destination address (board may have just been removed)
<b>Notice Log</b>	A connection that previously could not be closed has now closed; a multicast destination that previously could not be dropped has now been dropped
<b>Info</b>	Various logs to indicate events and transitions for low level diagnosis
<b>Debug</b>	Various logs to indicate events and transitions for low level diagnosis
<b>Filter</b>	None

## cops

---

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

**copsPr**


---

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

**coreDump**


---

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

**ctreeLog**


---

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

**dcm**


---

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



## dcmEngineGeneral

---

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

## dhcpCapture

---

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

**dhcpExternal**

---

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

**dhcpExternalEngine**

---

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

**dhcpGeneral**


---

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

**dhcplssuLog**


---

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

## dhcpLocalClients

---

<b>Description</b>	DHCP local server clients
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Cannot find the client's interface; cannot find the client to expire the lease or remove it from the database; trying to expire client's lease or remove it from database with bad IP address; requested MAC address does not match the available address; cannot allocate SDX subscriber information
<b>Warning Log</b>	Cannot find the DHCP instance for the client with an expired lease; cannot find the DHCP instance to release the client IP address; secondary DNS without primary DNS configured, using DHCP values; secondary NetBIOS Name Server (NBNS) without primary NBNS configured, using DHCP values
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Removing stale offers to clients and stale clients; adding and removing clients; expiring client's lease; client's transactions with DHCP local server
<b>Filter</b>	None

## dhcpLocalGeneral

---

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



**NOTE:** This category replaces the dhcpLocalServerGeneral category.

---

## dhcpLocalHighAvailability

---

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

## dhcpLocalPool

---

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

## dhcpLocalProtocol

---

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



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

---

**dhcpNvGeneral**

---

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

**dhcpOfferLog**

---

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



## dhcpPbeGeneral

---

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

## dhcpProxyGeneral

---

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

## dhcpRelayGeneral

---

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

## dhcpv6Client

---

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

**dhcpx6DemuxGeneral**

---

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

**dhcpx6LsGeneral**

---

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

## dismanEventMgr

---

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

## dnsGeneralLog

---

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

## dosProtection

---

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

## ds1

---

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

**ds3**


---

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

**dvmrpGeneral**


---

<b>Description</b>	DVMRP general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	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
<b>Warning Log</b>	Unable to add local route; routeHogCheck; routeLimit
<b>Notice Log</b>	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
<b>Info</b>	Designated forwarder election information; sending graft; timer expired for MulticastEntry; attempting to log duplicate accept filter; external route deleted or added
<b>Debug</b>	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

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

**dvmrpMcastTable**


---

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



**dvmrpProbeRcv**

---

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

**dvmrpProbeSent**

---

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

**dvmrpRtTable**


---

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

**ethernet**


---

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

## ethernetStateSession

---

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

## fileSystem

---

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

## flowInspection

---

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

## flowInspectionEngine

---

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

## flowServicesFirewallAlert

---

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

## flowServicesFirewallAudit

---

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

## frameRelay

---

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

## fsAgent

---

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

**ft1**


---

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

**ftpClient**


---

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

**ftpServer**


---

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

**gplaan**


---

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



**ha**


---

<b>Description</b>	High availability messages
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	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
<b>Warning Log</b>	High availability disabled due to incompatible release on standby; high availability disabled due to user initiated disable
<b>Notice Log</b>	High availability disabled due to standby down; high availability is now active
<b>Info</b>	None
<b>Debug</b>	None
<b>Filter</b>	None

**hdlc**


---

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

## hotfixGeneral

---

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

## httpServer

---

<b>Description</b>	Embedded HTTP server
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	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
<b>Warning Log</b>	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
<b>Notice Log</b>	None
<b>Info</b>	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
<b>Debug</b>	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
<b>Filter</b>	None

## iclImageFixServer

---

<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Memory allocation failure; ImageFix load failure; manual ImageFix activation failure; ImageFix file errors
<b>Warning Log</b>	Buffer allocation failure; unexpected status received in state X
<b>Notice Log</b>	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
<b>Info</b>	State machine change; unexpected internal communication error; loading complete announcement; IC up-to-date following SRP switch; sending ImageFix descriptor to line module
<b>Debug</b>	Controller state change announcement; board state change announcement; manual ImageFix [de]activation attempt; subsystem announced
<b>Filter</b>	None

## icmpTraffic

---

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

## icmpv6Traffic

---

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

## igmpGeneral

---

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



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

---

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



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

---

## igmpGracefulRestart

---

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



## igmpGroupState

---

<b>Description</b>	IGMP group state change events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	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)
<b>Debug</b>	None
<b>Filter</b>	router <i>virtualRouterName</i> [ interface <i>interfaceType</i> <i>interfaceSpecifier</i> ] <ul style="list-style-type: none"> <li>■ router—Logs events for a specific virtual router</li> <li>■ <i>virtualRouterName</i>—Name of the virtual router for which you want to log events</li> <li>■ interface—Logs events on a specific interface on the virtual router</li> <li>■ <i>interfaceType</i>—Type of the interface for which you want to log events. For example, atm or fastEthernet.</li> <li>■ <i>interfaceSpecifier</i>—Location of the interface in the appropriate format</li> </ul>



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

---

## ikeCertificateMgr

---

<b>Description</b>	Displays events relating to ERX key generation, certificate status, and certificate processing
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Initialization problems
<b>Warning Log</b>	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
<b>Notice Log</b>	Problem decoding certificates; IKE authentication problems related to certificates
<b>Info</b>	None
<b>Debug</b>	Certificate database notifications
<b>Filter</b>	None

## ikeEnrollment

---

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

**ikepki**


---

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

**interModuleCommunication**


---

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

## ipAccessList

---

<b>Description</b>	IP access list matching
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	Access list rule has been matched
<b>Debug</b>	None
<b>Filter 1:</b>	accessList <ul style="list-style-type: none"> <li>■ accessList—Logs a match on any access-list entry for all access lists</li> </ul>
<b>Filter 2:</b>	accessList router <i>virtualRouterName</i> access-list <i>accessListName</i> access-element-id <i>idNumber</i> <ul style="list-style-type: none"> <li>■ accessList—Logs a match on any access-list entry</li> <li>■ router—Logs events for a specific virtual router</li> <li>■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events</li> <li>■ access-list—Logs events for a specific access list</li> <li>■ <i>accessListName</i>—Name of access list for which you want to log events</li> <li>■ access-element-id—Logs events for a specific element ID</li> <li>■ <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 <b>show access-list detail</b> command</li> </ul>

## ipEngine

---

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

## ipflowstats

---

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

## ipflowstatsEngine

---

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

## ipGeneral

---

<b>Description</b>	IP general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	(IP) Interface stacking management errors
<b>Error</b>	(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
<b>Warning Log</b>	(IP) NVS load errors; failure to add address on an interface because of low memory
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	(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

<b>Description</b>	IP interface creator events
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	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
<b>Warning Log</b>	Client session already unbound; unable to process new configuration requests (out of resources)
<b>Notice Log</b>	Interface deletion failure in DCM (no client acknowledgement required)
<b>Info</b>	None
<b>Debug</b>	Client interaction during bind or unbind, session creation or shutdown, and interface creation or deletion; DCM interaction during interface creation or deletion
<b>Filter</b>	None

## ipInterface

---

<b>Description</b>	IP interface
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	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
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Interface state transitions and deletions; interface state machine events
<b>Filter 1:</b>	interface—See description of the ipGeneral interface filter for information about this filter
<b>Filter 2:</b>	router—See description of the ipGeneral router filter for information about this filter

## ipNhopTrackerGeneral

---

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



## ipProfileMgr

---

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

## ipRoutePolicy

---

<b>Description</b>	IP route policy
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	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
<b>Warning Log</b>	Failure to create a new routing policy due to memory limitation; misuse of a routing policy
<b>Notice Log</b>	None
<b>Info</b>	Result of routing policy check; specifies which routing policy is used
<b>Debug</b>	Successful addition or deletion of routing policies
<b>Filter</b>	router <i>virtualRouterName</i> <ul style="list-style-type: none"> <li>■ router—Logs IP route policy events for a specific virtual router</li> <li>■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events</li> </ul>

**ipRouteTable**


---

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

**ipseclDb**


---

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

## ipsecP1Throttler

---

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

## ipsecXcfgSM

---

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

**ipSubscriberMgr**

---

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

**ipTraffic**

---

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

## ipTunnel

---

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

## ipv6AccessList

---

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

## ipv6General

---

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

---

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

## ipv6ProfileMgr

---

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



## ipv6RouteTable

---

<b>Description</b>	IPv6 routing table
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Next-hop resolution-related problems; exceeding maximum route limit or warning threshold; route add and delete errors
<b>Warning Log</b>	Route limit-related warnings
<b>Notice Log</b>	Route limit-related messages
<b>Info</b>	None
<b>Debug</b>	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
<b>Filter 1:</b>	interface—See description of the ipv6General interface filter for information about this filter
<b>Filter 2:</b>	router—See description of the ipv6General router filter for information about this filter

## ipv6Traffic

---

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

## ipv6Types

---

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

---

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

## isisBfdEvents

---

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

## isisChecksumErr

---

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

## isisGeneral

---

<b>Description</b>	IS-IS system notifications
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error in restoring NVS
<b>Warning Log</b>	Exceeding maximum IP addresses on interface or maximum sequence number
<b>Notice Log</b>	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
<b>Info</b>	None
<b>Debug</b>	Redistributed routes
<b>Filter 1:</b>	interface—See description of the isisAdjChange interface filter for information about this filter
<b>Filter 2:</b>	router—See description of the isisAdjChange router filter for information about this filter

## isisHelloGeneral

---

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

## isisHelloPackets

---

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

## isisIpv6Log

---

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

## isisLdpEvents

---

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



## isisLocalUpdate

---

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

## isisMplsTeAdvertisements

---

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

## isisMplsTeEvents

---

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

## isisNsfEvents

---

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

## isisProtocolErr

---

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

## isisSnpPackets

---

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

## isisSpfEvents

---

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

## isisSpfStatistics

---

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

## isisSpfTriggers

---

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

## isisUpdatePackets

---

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

**isVoice**


---

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

**itm**


---

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

## I2cGeneral

---

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

## I2cKeepAlive

---

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

## I2cPacket

---

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

## I2tp

---

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



## I2tpDialoutGenerator

---

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

## I2tpDisconnectCause

---

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

## I2tpIpLowerBinding

---

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

## I2tpStateMachine

---

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

## IdpConnect

---

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

## IdpGeneral

---

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

## IdpGracefulRestart

---

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

## IdpHelloMessages

---

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

## IdpHelloMgr

---

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

## ldpInterface

---

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



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

---

## IdpMessages

---

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

## IdpPeer

---

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

## ldpShimInterface

---

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



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

---



## IdpSocket

---

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

## IdpTimer

---

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

## IdpVpls

---

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

## IdpWorker

---

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

## localAddressServerGeneral

---

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

## localAuthServer

---

<b>Description</b>	Local authentication server
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	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
<b>Warning Log</b>	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
<b>Notice Log</b>	None
<b>Info</b>	None
<b>Debug</b>	Server started; server bind occurred; no user name provided; no CHAP challenge provided; no authenticate request message allocated
<b>Filter</b>	None

## localEnableAuthServer

---

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

## localLinePassword

---

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

## macroData

---

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

## mgmtGeneral

---

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



**NOTE:** For information about interface types and specifiers, see *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

---

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

## mgtmv6General

---

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

---

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



## mldGeneral

---

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

---

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

## mldGroupState

---

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



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

---

**mmcd**


---

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

**mobileipv4HaBinding**


---

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

## mobileIpv4HaEng

---

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

## mobileIpv4HaEvent

---

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

## mobileIpv4HaLog

---

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

## mplsFwdTable

---

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

## mplsGeneral

---

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

## mplsHighAvailability

---

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

## mplsMajorInterface

---

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



**NOTE:** For information about interface types and specifiers, see *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

---

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

## mplsShimInterface

---

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



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

---

**mplsTraffic**


---

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

**mrInfoLog**


---

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

## mrInfoRcvdLog

---

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

## mrInfoSentLog

---

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

## mtraceLog

---

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

## mtraceRcvdLog

---

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

## mtraceSentLog

---

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

## multicastTraffic

---

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



## nameResolverLog

---

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

## nfsClient

---

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

## noneAaaAddrServer

---

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

## noneAaaServer

---

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

## ntpGeneral

---

<b>Description</b>	Network Time Protocol (NTP) system notifications
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	NVS configuration errors; insufficient memory resources; protocol errors; time adjustment failures
<b>Warning Log</b>	No usable servers, NTP synchronization lost
<b>Notice Log</b>	System time adjustment
<b>Info</b>	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
<b>Debug</b>	None
<b>Filter</b>	router ID

**OS**


---

<b>Description</b>	Operating system (including image loader)
<b>Emergency</b>	None
<b>Alert</b>	Fatal software error notification (assertions, panics, exceptions); panic timer expiration; ECC memory errors
<b>Critical</b>	System halt; NVS reverting to factory defaults
<b>Error</b>	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
<b>Warning Log</b>	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
<b>Notice Log</b>	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)
<b>Info</b>	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
<b>Debug</b>	High-frequency debug messages (enabled with various build defines); cached file hit, miss, or close; image loader frame retry; NVS config cache flush status
<b>Filter</b>	None

## ospfElectDr

---

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



**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

<b>Description</b>	OSPF general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Error enabling or disabling OSPF; allocation errors
<b>Warning Log</b>	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
<b>Notice Log</b>	OSPF enabled or disabled; BFD enabled or disable on an OSPF interface
<b>Info</b>	Event for a dynamic neighbor
<b>Debug</b>	Bouncing adjacency with a neighbor
<b>Filter 1:</b>	interface-ip-address—See description of the ospfElectDr interface-ip-address filter for information about this filter
<b>Filter 2:</b>	router—See description of the ospfElectDr router filter for information about this filter

## ospfHelloPktsRcvd

---

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



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

---

**ospfHelloPktsSent**

---

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



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

---



## ospfInterface

---

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

## ospfLdpEvents

---

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

**ospfLsa**


---

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

## ospfNeighbor

---

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

## ospfPktsRcvd

---

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

**ospfPktsSent**

---

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

**ospfRestart**

---

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

## ospfRoute

---

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

## ospfSpfExt

---

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

## ospfSpfInter

---

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

## ospfSpfIntra

---

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

## ospfTeDatabase

---

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

## ospfTeSpf

---

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

**ospfv3ElectDr**


---

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

---



**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

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

**ospfv3HelloPktsRcvd**

---

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

## ospfv3HelloPktsSent

---

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

## ospfv3Interface

---

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

**ospfV3Lsa**


---

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

## ospfv3Neighbor

---

<b>Description</b>	OSPFv3 neighbor change
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Neighbor MTU negotiation rejects
<b>Warning Log</b>	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
<b>Notice Log</b>	Database description neighbor exchange; neighbor state changes; neighbor retransmissions
<b>Info</b>	None
<b>Debug</b>	Router exits graceful restart; helping router with graceful restart
<b>Filter 1:</b>	neighbor—See description of the ospfLsa neighbor filter for information about this filter
<b>Filter 2:</b>	router—See description of the ospfLsa router filter for information about this filter

## ospfv3PktsRcvd

---

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

## ospfv3PktsSent

---

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

**ospfv3Route**

---

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

**ospfV3SpfExt**

---

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



## ospfV3SpfInter

---

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

## ospfV3SpfIntra

---

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

**pimAutoRPRcvdLog**


---

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

---



**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 unnumbered interface in the appropriate format



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

---

## pimAutoRPSentLog

---

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

**pimBsrRcvdLog**

---

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

**pimBsrSentLog**

---

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

## pimGracefulRestartLog

---

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

## pimHelloRcvdLog

---

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

## pimHelloSentLog

---

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

## pimIpv6AutoRPRcvdLog

---

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

- *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

---

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

## pimIpv6BsrRcvdLog

---

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



## pimIpv6BsrSentLog

---

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

## pimIpv6GracefulRestartLog

---

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

**pimIpv6HelloRcvdLog**


---

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

---



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

---

<b>Filter 2:</b>	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"> <li>■ router—Logs events for a specific virtual router</li> <li>■ <i>virtualRouterName</i>—Name of virtual router for which you want to log events</li> <li>■ interface-ipv6-address—Logs events for a specific interface on the virtual router</li> <li>■ ipv6-address—Specifies that you will identify the interface by entering an IPv6 address</li> <li>■ <i>ipv6Address</i> —IPv6 address of interface for which you want to log events</li> <li>■ unnumbered—Specifies that the interface is unnumbered</li> </ul>
------------------	--

- *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

---

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

## pimIpv6PktsRcvdLog

---

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

## pimIpv6PktsSentLog

---

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

## pimPktsRcvdLog

---

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

## pimPktsSentLog

---

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

**pimsmGeneral**


---

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

**pimsmMvpn**


---

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

## policyMgrAttachment

---

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

## policyMgrGeneral

---

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

**policyMgrPacketLog**


---

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

**ppp**


---

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



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

---



**pppoe**


---

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

---



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

---

## pppoeControlPacket

---

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



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

---

## pppPacket

---

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



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

---

## pppStateMachine

---

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



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

---

**profileMgr**


---

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

**qm**


---

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

**qos**


---

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

**qosAttachment**


---

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

## radiusAttributes

---

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

## radiusClient

---

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

**radiusCoAAttributes**


---

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

**radiusDisconnectGeneral**


---

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



## radiusRelayGeneral

---

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

## radiusSendAttributes

---

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

**remOps**


---

<b>Description</b>	Remote operations
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Internal error
<b>Warning Log</b>	Maximum table size reached; ICMP failure; same target probed by more than one entry
<b>Notice Log</b>	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
<b>Info</b>	None
<b>Debug</b>	Ping, traceroute, or nslookup session begin or end; packet receive; duplicate receive
<b>Filter</b>	None

**resourceThresholdTrap**


---

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

**ripBfd**

---

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

## ripGeneral

---

**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

---

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



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

---

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

**ripRtTable**


---

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

**routeDownloader**


---

<b>Description</b>	RADIUS route-download server operation
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Unable to create application process when configured
<b>Warning Log</b>	Write to mirrored storage memory failed
<b>Notice Log</b>	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; <b>clear all</b> command is terminated due to download failure; empty download
<b>Info</b>	Download started, completed, or finalized; IP update started, completed, or finalized
<b>Debug</b>	Download operation information; such as download request sent. download response received
<b>Filter</b>	None

## routerLog

---

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

## rsvpAsyncMgr

---

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

**rsvpBfd**


---

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

**rsvpGeneral**


---

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



## **rsvpGracefulRestart**

---

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

## rsvpInterface

---

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



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

---

## rsvpTunnel

---

<b>Description</b>	RSVP tunnels
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Critical operational errors
<b>Error</b>	Operational errors; resource allocation failures
<b>Warning Log</b>	Operational failures; fast-reroute triggering
<b>Notice Log</b>	Less serious operational failures; network changes
<b>Info</b>	Minor internal errors; timer operations
<b>Debug</b>	Function flows, parameter passing
<b>Filter</b>	router <i>virtualRouterName</i> <ul style="list-style-type: none"> <li>■ router—Logs events for traffic on a specific virtual router</li> <li>■ <i>virtualRouterName</i>—Name of virtual router</li> </ul>

## security

---

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

## serviceability

---

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

## serviceMgr

---

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

## serviceMgrClientSession

---

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

## serviceMgrDcm

---

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

## serviceMgrMacroManager

---

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

## serviceMgrPerformance

---

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

**serviceMgrServiceDef**

---

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

**serviceMgrServiceInstance**

---

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

## serviceMgrServiceSession

---

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

## serviceMgrSubscriberSession

---

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



**slep**


---

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

---



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

---

**snmp**


---

<b>Description</b>	Embedded SNMP agent
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	Access violation due to underprivileged community string or a bad proxy selector; access denial due to configured access list; configuration of SNMP failed; trap is dropped because of the severity level filter or because the trap category is not enabled
<b>Notice Log</b>	None
<b>Info</b>	SNMP agent has been enabled or disabled
<b>Debug</b>	Trap request dropped; trap processing summary statistics
<b>Filter</b>	None

---

**snmpIfMib**


---

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

**snmpPduAudit**


---

<b>Description</b>	SNMP PDUs
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	Identifies the following fields in all SNMP PDUs sent to the E-series router and all trap PDUs that leave the system: source and destination IP address, PDU type, snmpVersion, requested, errorStatus, errorIndex, variable count, variable object identifier and data
<b>Debug</b>	None
<b>Filter</b>	None

## snmpSetPduAudit

---

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

## snmpTrap

---

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

**sonet**


---

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

**sonetPath**


---

<b>Description</b>	SONET Path
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	None
<b>Warning Log</b>	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
<b>Notice Log</b>	Pool expansion
<b>Info</b>	Init from NV failures; NV upgrade; path update progress; path configuration notification
<b>Debug</b>	Path update
<b>Filter</b>	None

**sonetVT**


---

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

**ssccDetailPm**


---

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

**ssccDetailSsc**


---

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

**ssccGeneral**


---

<b>Description</b>	SDX client (formerly SSCC) general
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	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
<b>Warning Log</b>	None
<b>Notice Log</b>	None
<b>Info</b>	Creation or deletion of SDX client
<b>Debug</b>	Events (create interface, reports, removals); policy deletions; policy reattachments; CLI events; connection retries
<b>Filter</b>	None

**ssh**


---

<b>Description</b>	Secure Shell (SSH) Server
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Cannot create SSH daemon; unexpected socket condition; packet overrun; AAA failure; resource allocation failure; host key read error
<b>Warning Log</b>	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
<b>Notice Log</b>	AAA user authentication failure; ignored channel request; client connect/disconnect
<b>Info</b>	Detailed client connection info (per connection attempt)
<b>Debug</b>	Daemon instance creation/removal; detailed packet info (per packet)
<b>Filter</b>	None

**stTunnel**


---

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

## stTunnelEngine

---

<b>Description</b>	Logs events and conditions related to the communication between the IPSec tunnels application and the IPSec server and line modules
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	None
<b>Error</b>	Unexpected and nonrecoverable communication errors
<b>Warning Log</b>	Unexpected but recoverable events
<b>Notice Log</b>	Controller up/down and restart up/down events
<b>Info</b>	Processing of controller up/down and restart up/down events; processing of synchronization events following a cold- or warm-restart
<b>Debug</b>	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
<b>Filter</b>	None



**system**


---

<b>Description</b>	System management and monitoring
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Line module ping failure threshold exceeded; test failure on line module or standby SRP module; test failure on line module or standby SRP module
<b>Error</b>	Error on line module or standby SRP module; 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
<b>Warning Log</b>	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
<b>Notice Log</b>	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
<b>Info</b>	Synchronization start, complete; line module set timing failed (not necessarily an error); NVS volume flush
<b>Debug</b>	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
<b>Filter</b>	slot <i>slotNumber</i> <ul style="list-style-type: none"> <li>■ slot—Logs events for a specific slot</li> <li>■ <i>slotNumber</i>—Number of slot for which you want to log events</li> </ul>

## tacacsPlusServer

---

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

## tcpGeneral

---

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

## tcpTraffic

---

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

## tcpv6Traffic

---

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

**telnet**


---

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

**telnetClient**


---

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

**tftpClient**

---

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

**trackerEvents**

---

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

## trackerGeneral

---

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

## tsm

---

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

## udpTraffic

---

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



## udpv6Traffic

---

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

**vrrp**


---

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

---



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

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

## vrrpTracking

---

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

## vsm

---

<b>Description</b>	VLAN subinterface manager
<b>Emergency</b>	None
<b>Alert</b>	None
<b>Critical</b>	Unable to find VLAN major interface for agent-circuit-id-based VLAN
<b>Error</b>	Truncating agent-circuit-id string
<b>Warning Log</b>	Creation failure
<b>Notice Log</b>	Out of pool space
<b>Info</b>	Replay of unknown interface after high availability switchover
<b>Debug</b>	General VSM operations, such as agent-circuit-id-based VLAN created
<b>Filter</b>	None

**vsmEngine**

---

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

# 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 ..... 7  
log severity ..... 7  
log unlimit ..... 8  
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	ipsecIdDb .....	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
dhcpv6Client .....	60	ipv6Interface .....	98
dhcpv6DemuxGeneral .....	61	ipv6ProfileMgr .....	98
dhcpv6LsGeneral .....	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	l2tpIpLowerBinding .....	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	<b>N</b>	
rsvpGeneral .....	202	notice icons defined .....	xiv
rsvpGracefulRestart .....	203	<b>P</b>	
rsvpInterface .....	204	platform considerations	
rsvpTunnel .....	205	system logs .....	3
security .....	205	<b>R</b>	
serviceability .....	206	release notes .....	xviii
serviceMgr .....	206	<b>S</b>	
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 .....	18
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 .....	18
sonetPath .....	214	<b>T</b>	
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		
<b>M</b>			
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		