JUNOS® Software

System Log Messages Reference

Release 9.4

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-028727-01, Revision 1

JUNOS® Software System Log Messages Reference
Release 9.4

Writing: Paka Sheryll Marion Sampson
Editing: Nancy Kurahashi
Cover Design: Edmonds Design

Revision History
15th January 2009—Revision 1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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 (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) 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, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the 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 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 or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations 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 Embedded Software on non-Juniper equipment; (j) use Embedded 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 NONINFRINGEMENT. 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 payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

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 présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

Part 3 Index

Table of Contents

About This Guide

This preface provides the following guidelines for using the *JUNOS® Software System Log Messages Reference*:

Objectives

This reference describes system log messages generated by the JUNOS software. Use the information to interpret system log messages and determine the appropriate corrective action for error conditions

NOTE: This guide documents Release 9.4 of the JUNOS software. For additional information about the JUNOS software—either corrections to or information that might have been omitted from this guide—see the software release notes at http://www.juniper.net/.

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M-series, MX-series, T-series, EX-series, or J-series router or switch.

To use this reference, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)

- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

Supported Platforms

For the features described in this manual, the JUNOS software currently supports the following platforms:

- J-series
- M-series
- MX-series
- T-series
- EX-series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the load merge or the load merge relative command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the load merge command

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the load merge relative command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file ex-script.conf. Copy the ex-script.conf file to the /var/tmp directory on your routing platform.

```
system {
  scripts {
   commit {
    file ex-script.xsl;
   }
  }
}
interfaces {
  fxp0 {
   disable;
   unit 0 {
    family inet {
     address 10.0.0.1/24;
    }
   }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the load merge configuration mode command:

```
[edit]
user@host#  load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file ex-script-snippet.conf. Copy the ex-script-snippet.conf file to the /var/tmp directory on your routing platform.

```
commit {
file ex-script-snippet.xsl;
}
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the load merge relative configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the load command, see the *JUNOS CLI User Guide*

Documentation Conventions

Table 1 on page lvi 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 or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page lvi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic text like this	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric *metric*>;
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast | multicast (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [*community-ids*]

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	■ In the Logical Interfaces box, select **All Interfaces**. ■ To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols > Ospf**.

List of Technical Publications

Table 3 on page lviii lists the software and hardware guides and release notes for Juniper Networks M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 4 on page lxii lists the books included in the

Network Operations Guide series. Table 5 on page lxii lists the manuals and release notes supporting JUNOS software for J-series and SRX-series platforms. All documents are available at http://www.juniper.net/techpubs/.

Table 6 on page lxiii lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at http://www.juniper.net/books.

Table 3: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	
Access Privilege	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
Broadband Subscriber Management Solutions	Describes residential subscriber management and how you can deploy solutions that include multisubscriber IP address assignment, service provisioning, authentication, authorization, accounting, and dynamic request services in your network
Class of Service	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
CLI User Guide	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
High Availability	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES).
MPLS Applications	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
Multicast Protocols	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
Multiplay Solutions	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.

Table 3: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
MX-series Layer 2 Configuration Guide	Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the *JUNOS Routing Protocols Configuration Guide*.
MX-series Layer 2 Solutions Guide	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
Network Interfaces	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
Network Management	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
Policy Framework	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
Protected System Domain	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
Routing Protocols	Provides an overview of routing concepts and describes how to configure routing instances, and unicast routing protocols.
Secure Configuration Guide for Common Criteria and JUNOS-FIPS	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
Services Interfaces	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
Software Installation and Upgrade Guide	Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
Subscriber Access	Provides an overview of the subscriber access features of the JUNOS software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods.

Table 3: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
System Basics	Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
VPNs	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
Hierarchy and RFC Reference	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
Interfaces Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
Routing Protocols and Policies Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
System Basics and Services Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPsec), stateful firewalls, flow collection, and flow monitoring.
System Log Messages Reference	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
J-Web Interface User Guide	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
JUNOScript API Guide	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
JUNOS XML API Configuration Reference	Provides reference pages for the configuration tag elements in the JUNOS XML API.
JUNOS XML API Operational Reference	Provides reference pages for the operational tag elements in the JUNOS XML API.
NETCONF API Guide	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.

Table 3: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
JUNOS Configuration and Diagnostic Automation Guide	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
Hardware Documentation	
Hardware Guide	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
PIC Guide	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
DPC Guide	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Advanced Insight Solutions (AIS) Documentation	
Advanced Insight Solutions Guide	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.
Release Notes	
JUNOS Release Notes	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
Hardware Release Notes	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
JUNOScope Release Notes	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
AIS Release Notes	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
AIS AI-Scripts Release Notes	Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.

Table 4: JUNOS Software Network Operations Guides

Book	Description
Baseline	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
Interfaces	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
MPLS	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
MPLS Log Reference	Describes MPLS status and error messages that appear in the output of the show mpls lsp extensive command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
MPLS Fast Reroute	Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing.
Hardware	Describes tasks for monitoring M-series and T-series routing platforms.

To configure and operate a J-series Services Router or an SRX-series Services Gateway running JUNOS software, you must also use the configuration statements and operational mode commands documented in JUNOS configuration guides and command references. To configure and operate a WX Integrated Services Module, you must also use WX documentation.

Table 5: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation

Book	Description
J-series and SRX-series Platforms	
JUNOS Software Interfaces and Routing Configuration Guide	Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
JUNOS Software Security Configuration Guide	Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).

Table 5: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation *(continued)*

Book	Description
JUNOS Software Administration Guide	Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
JUNOS Software CLI Reference	Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices.
JUNOS Release Notes	Summarize new features and known problems for a particular release of JUNOS software, including JUNOS software for J-series and SRX-series devices.The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software.
J-series Only	
JUNOS Software Design and Implementation Guide	Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software.
J-series Services Routers Quick Start	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
J-series Services Router Hardware Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
JUNOS Software Migration Guide	Provides instructions for migrating an SSG device running ScreenOS software to JUNOS software or upgrading a J-series device to a later version of the JUNOS software.
WXC Integrated Services Module Installation and Configuration Guide	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.

Table 6: Additional Books Available Through http://www.juniper.net/books

Book	Description
Interdomain Multicast Routing	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.

Table 6: Additional Books Available Through http://www.juniper.net/books *(continued)*

Book	Description
JUNOS Cookbook	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
MPLS-Enabled Applications	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.
OSPF and IS-IS: Choosing an IGP for Large-Scale Networks	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks.
Routing Policy and Protocols for Multivendor IP Networks	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.
The Complete IS-IS Protocol	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs])*

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 postsales 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 Management tool: 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 Management 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 us at http://www.juniper.net/support/requesting-support.html.

Part 1
Overview

Chapter 1

Configuring System Log Messages

The JUNOS software generates system log messages (also called syslog messages) to record events that occur on the routing platform, including the following:

- Routine operations, such as creation of an OSPF protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a peer process
- Emergency or critical conditions, such as routing platform power-down due to excessive temperature

Each system log message identifies the JUNOS software process that generated the message and briefly describes the operation or error that occurred. This reference provides more detailed information about each system log message and, when applicable, describes possible causes of the message and action you can take to correct error conditions.

NOTE: The configuration hierarchy in this chapter applies to JUNOS software processes and libraries, not to the services on a Physical Interface Card (PIC) such as the Adaptive Services PIC. For information about configuring system logging for PIC services, see the *JUNOS Services Interfaces Configuration Guide*.

For information about interpreting messages generated by services on a PIC, see "Interpreting Messages Generated in Standard Format by Services on a PIC" on page 44.

This chapter discusses the following topics:

System Logging Configuration Statements

To configure the routing platform to log system messages, include the **syslog** statement at the [**edit system**] hierarchy level:

```
[edit system]
syslog {
 archive {
  files number;
  size size;
  (world-readable | no-world-readable);
 }
 console {
 facility severity;
 }
 file filename {
  facility severity;
  explicit-priority;
  match "regular-expression";
  structured-data {
   brief;
  }
  archive {
   files number;
   size size;
   (world-readable | no-world-readable);
  }
 }
 host (hostname | other-routing-engine | scc-master) {
  facility severity;
  explicit-priority;
  facility-override facility;
  log-prefix string;
  match "regular-expression";
 }
 source-address source-address;
 time-format (year | millisecond | year millisecond);
 user (username | *) {
  facility severity;
  match "regular-expression";
 }
}
```

Minimum and Default System Logging Configuration

For information about the minimum and default system log settings on routing platforms that run the JUNOS software, see the following sections:

- Minimum System Logging Configuration on page 5
- Default System Log Settings on page 5

Minimum System Logging Configuration

To record or view system log messages, you must include the syslog statement at the [edit system] hierarchy level. Specify at least one destination for the messages, as described in Table 7 on page 5. For more information about the configuration statements, see "Configuring System Logging for a Single-Chassis System" on page 7.

Table 7: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration Statements

File	[edit system syslog]
	file *filename* {
	facility severity ;
	}

Terminal session of one, several, or all users	[edit system syslog]
	user (*username* | *) {
	facility severity ;
	}

Routing platform console	[edit system syslog]
	console {
	facility severity ;
	}

Remote machine or the other Routing Engine on the routing platform	[edit system syslog]
	host (*hostname* | other-routing-engine) {
	facility severity ;
	}

Default System Log Settings

Table 8 on page 6 summarizes the default system log settings that apply to all platforms that run the JUNOS software, and specifies which statement to include in the configuration to override the default value.

Table 8: Default System Logging Settings

Setting	Default	Overriding Statement	Instructions

Alternative facility for message forwarded to a remote machine	For change-log: local6
	
	For conflict-log: local5
	
	For dfc: local1
	
	For firewall: local3
	
	For interactive-commands: local7
	
	For pfe: local4
		[edit system syslog]
		host *hostname* {
		facility-override *facility*;
		}
			"Changing the Alternative Facility Name for Remote Messages" on page 14

Format of messages logged to a file	Standard JUNOS format, based on UNIX format	[edit system syslog]
		file *filename* {
		structured-data;
		}
			"Logging Messages in Structured-Data Format" on page 12

Maximum number of files in the archived set	10	[edit system syslog]
		archive {
		files *number*;
		}
		file *filename* {
		archive {
		files *number* ;
		}
		}
			"Configuring the Size and Number of Log Files" on page 18

Maximum size of log file	J-series: 128 kilobytes (KB)
	
	M-series, MX-series, and T-series: 1 megabyte (MB)
	
	TX Matrix: 10 MB
		[edit system syslog]
		archive {
		size *size*;
		}
		file *filename* {
		archive {
		size *size*;
		}
		}
			"Configuring the Size and Number of Log Files" on page 18

Timestamp format	Month, date, hour, minute, second For example: **Aug 21 12:36:30**	[edit system syslog] time-format *format*;	"Including the Year or Millisecond in Timestamps" on page 22

Users who can read log files	root user and users with the JUNOS maintenance permission	[edit system syslog]
		archive {
		world-readable;
		}
		file *filename* {
		archive {
		world-readable;
		}
		}
			"Configuring the Size and Number of Log Files" on page 18

In addition, the following messages are generated by default on specific platforms. To view either type of message, you must configure at least one destination for messages as described in "Minimum System Logging Configuration" on page 5

- On J-series platforms, a message is logged when a process running in the kernel consumes 500 or more consecutive milliseconds of CPU time.

  To log the message on an M-series, MX-series, or T-series platform, include the **kernel info** statement at the appropriate hierarchy level:

  ```
  [edit system syslog]
  (console | file filename | host destination | user username) {
   kernel info;
  }
  ```

- The master Routing Engine on each T640 routing node in a routing matrix forwards to the master Routing Engine on the TX Matrix platform all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix platform:

  ```
  [edit system syslog]
  host scc-master {
   any info;
  }
  ```

Configuring System Logging for a Single-Chassis System

The JUNOS system logging utility is similar to the UNIX **syslogd** utility. This section describes how to configure system logging for a single-chassis system that runs the JUNOS software.

System logging configuration for the JUNOS-FIPS software and for Juniper Networks routing platforms in a Common Criteria environment is the same as for the JUNOS software. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

For information about configuring system logging for a routing matrix, see "Configuring System Logging for a Routing Matrix" on page 28.

Each system log message belongs to a facility, which groups together related messages. Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects routing platform functions. You always specify the facility and severity of the messages to include in the log. For more information, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 9.

You direct messages to one or more destinations by including the appropriate statement at the [edit system syslog] hierarchy level:

- To a named file in a local file system, by including the file statement. See "Directing Messages to a Log File" on page 11.
- To the terminal session of one or more specific users (or all users) when they are logged in to the routing platform, by including the user statement. See "Directing Messages to a User Terminal" on page 12.
- To the routing platform console, by including the console statement. See "Directing Messages to the Console" on page 13.
- To a remote machine that is running the syslogd utility or to the other Routing Engine on the routing platform, by including the host statement. See "Directing Messages to a Remote Machine or the Other Routing Engine" on page 13.

By default, messages are logged in a standard format, which is based on a UNIX system log format; for detailed information, see "Interpreting System Log Messages" on page 38. You can alter the content and format of logged messages in the following ways:

- In JUNOS 8.3 and later, you can log messages to a file in structured-data format instead of the standard JUNOS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from the message. For more information, see "Logging Messages in Structured-Data Format" on page 12.
- A message's facility and severity level are together referred to as its priority. By default, the standard JUNOS format for messages does not include priority information. (Structured-data format includes a priority code by default.) To include priority information in standard-format messages directed to a file or a remote destination, include the explicit-priority statement. For more information, see "Including Priority Information in System Log Messages" on page 19.
- By default, the standard JUNOS format for messages specifies the month, date, hour, minute, and second when the message was logged. You can modify the timestamp on standard-format messages to include the year, the millisecond, or both. (Structured-data format specifies the year and millisecond by default.) For more information, see "Including the Year or Millisecond in Timestamps" on page 22.
- When directing messages to a remote machine, you can specify the IP address that is reported in messages as their source. You can also configure features that make it easier to separate JUNOS-specific messages or messages generated on particular routing platforms. For more information, see "Directing Messages to a Remote Machine or the Other Routing Engine" on page 13.
- The predefined facilities group together related messages, but you can also use regular expressions to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination. For more information, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 23.

For a statement summary for the statements discussed in this chapter, see the *JUNOS System Basics Configuration Guide*.

For detailed information about configuring system logging, see the following sections:

Specifying the Facility and Severity of Messages to Include in the Log

Each system log message belongs to a facility, which groups together messages that either are generated by the same source (such as a software process) or concern a similar condition or activity (such as authentication attempts). Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects routing platform functions.

When you configure logging for a facility and destination, you specify a severity level for each facility. Messages from the facility that are rated at that level or higher are logged to the destination

```
[edit system syslog]
(console | file filename | host destination | user username) {
 facility severity ;
}
```

(For information about the destinations, see “Directing Messages to a Log File” on page 11,“Directing Messages to a User Terminal” on page 12,“Directing Messages to the Console” on page 13 and “Directing Messages to a Remote Machine or the Other Routing Engine” on page 13.)

To log messages belonging to more than one facility to a particular destination, specify each facility and associated severity as a separate statement within the set of statements for the destination.

Table 9 on page 9 lists the facilities that you can specify in configuration statements at the [edit system syslog] hierarchy level.

Table 9: JUNOS System Logging Facilities

Facility	Type of Event or Error
any	All (messages from all facilities)
authorization	Authentication and authorization attempts

Table 9: JUNOS System Logging Facilities *(continued)*

Facility	Type of Event or Error
change-log	Changes to the JUNOS configuration
conflict-log	Specified configuration is invalid on the routing platform type
daemon	Actions performed or errors encountered by system processes
dfc	Events related to dynamic flow capture
firewall	Packet filtering actions performed by a firewall filter
ftp	Actions performed or errors encountered by the FTP process
interactive-commands	Commands issued at the JUNOS command-line interface (CLI) prompt or invoked by a client application such as a JUNOScript or NETCONF client
kernel	Actions performed or errors encountered by the JUNOS kernel
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
user	Actions performed or errors encountered by user-space processes

Table 10 on page 10lists the severity levels that you can specify in configuration statements at the [edit system syslog] hierarchy level. The levels from emergency through info are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the none level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see “Disabling Logging of a Facility” on page 25

Table 10: System Log Message Severity Levels

Severity Level	Description
any	Includes all severity levels
none	Disables logging of the associated facility to a destination
emergency	System panic or other condition that causes the routing platform to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database

Table 10: System Log Message Severity Levels *(continued)*

Severity Level	Description
critical	Critical conditions, such as hard drive errors
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or nonerror conditions of interest

Directing Messages to a Log File

To direct system log messages to a file in the /var/log directory of the local Routing Engine, include the file statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
file filename {
 facility severity ;
 explicit-priority;
 match "regular-expression";
 structured-data {
  brief;
 }
 archive {
  files number ;
  size size;
  (world-readable | no-world-readable);
 }
}
```

For the list of facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 9.

To prevent log files from growing too large, the JUNOS system logging utility by default writes messages to a sequence of files of a defined size. By including the archive statement, you can configure the number of files, their maximum size, and who can read them, for either all log files or a certain log file. For more information, see "Configuring the Size and Number of Log Files" on page 18.

For information about the following statements, see the indicated sections:

- explicit-priority—See "Including Priority Information in System Log Messages" on page 19.
- match—See "Using Regular Expressions to Refine the Set of Logged Messages" on page 23.

- structured-data—See "Logging Messages in Structured-Data Format" on page 12.

Logging Messages in Structured-Data Format

In JUNOS 8.3 and later, you can log messages to a file in structured-data format instead of the standard JUNOS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from a message.

The structured-data format complies with Internet draft draft-ietf-syslog-protocol-21.txt, *The syslog Protocol*, which at the time of this writing is accessible at http://www.ietf.org/internet-drafts/draft-ietf-syslog-protocol-21.txt. The draft establishes a standard message format regardless of the source or transport protocol for logged messages.

To output messages to a file in structured-data format, include the structured-data statement at the [edit system syslog file *filename*] hierarchy level:

```
[edit system syslog file filename]
facility severity;
structured-data {
 brief;
}
```

The optional brief statement suppresses the English-language text that appears by default at the end of a message to describe the error or event. For information about the fields in a structured-data–format message, see "Displaying a Log File from a Single-Chassis System" on page 37

The structured format is used for all messages logged to the file that are generated by a JUNOS process or software library.

NOTE: If you include either or both of the explicit-priority and time-format statements along with the structured-data statement, they are ignored. These statements apply to the standard JUNOS system log format, not to structured-data format.

Directing Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged in to the local Routing Engine, include the user statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
user (username | *) {
 facility severity;
 match "regular-expression";
}
```

Specify one or more JUNOS usernames, separating multiple values with spaces, or use the asterisk (*) to indicate all users who are logged in to the local Routing Engine.

For the list of facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 9. For information about the match statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 23

Directing Messages to the Console

To direct system log messages to the console of the local Routing Engine, include the console statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
console {
 facility severity;
}
```

For the list of facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 9.

Directing Messages to a Remote Machine or the Other Routing Engine

To direct system log messages to a remote machine or to the other Routing Engine on the routing platform, include the host statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
host (hostname | other-routing-engine) {
 facility severity;
 explicit-priority;
 facility-override facility;
 log-prefix string;
 match "regular-expression";
}
source-address source-address;
```

To direct system log messages to a remote machine, include the host *hostname* statement to specify the remote machine's IP version 4 (IPv4) address, IP version 6 (IPv6) address, or fully qualified hostname. The remote machine must be running the standard syslogd utility. We do not recommend directing messages to another Juniper Networks routing platform. In each system log message directed to the remote machine, the hostname of the local Routing Engine appears after the timestamp to indicate that it is the source for the message.

To direct system log messages to the other Routing Engine on a routing platform with two Routing Engines installed and operational, include the host other-routing-engine statement. The statement is not automatically reciprocal, so you must include it in each Routing Engine's configuration if you want them to direct messages to each other. In each message directed to the other Routing Engine, the string re0 or re1 appears after the timestamp to indicate the source for the message.

For the list of facilities and severity levels to configure under the host statement, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 9.

To record facility and severity level information in each message, include the explicit-priority statement. For more information, see "Including Priority Information in System Log Messages" on page 19.

For information about the match statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 23.

When directing messages to remote machines, you can include the source-address statement to specify the IP address of the routing platform that is reported in the messages as their source. In each host statement, you can also include the facility-override statement to assign an alternative facility and the log-prefix statement to add a string to each message. For more information, see the following sections:

- Specifying an Alternative Source Address for System Log Messages on page 14
- Changing the Alternative Facility Name for Remote Messages on page 14
- Examples: Assigning an Alternative Facility on page 16
- Adding a Text String to System Log Messages on page 17
- Adding a String on page 17

Specifying an Alternative Source Address for System Log Messages

To specify the routing platform that is reported in system log messages as their source when they are directed to a remote machine, include the source-address statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
source-address source-address;
```

source-address is a valid IPv4 or IPv6 address configured on one of the routing platform interfaces. The address is reported in the messages directed to all remote machines specified in host *hostname* statements at the [edit system syslog] hierarchy level, but not in messages directed to the other Routing Engine.

Changing the Alternative Facility Name for Remote Messages

Some facilities assigned to messages logged on the local routing platform have JUNOS-specific names (see Table 9 on page 9 in "Specifying the Facility and Severity of Messages to Include in the Log" on page 9. In the recommended configuration, a remote machine designated at the [edit system syslog host hostname] hierarchy level is not a Juniper Networks routing platform, so its syslogd utility cannot interpret the JUNOS-specific names. To enable the standard syslogd utility to handle messages from these facilities, when messages are directed to a remote machine a standard localX facility name is used instead of the JUNOS-specific facility name.

Table 11 on page 15 lists the default alternative facility name used for each JUNOS-specific facility name. For facilities that are not listed, the default alternative name is the same as the local facility name.

Table 11: Default Facilities for Messages Directed to a Remote Destination

JUNOS-Specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6
conflict-log	local5
dfc	local1
firewall	local3
interactive-commands	local7
pfe	local4

The syslogd utility on a remote machine handles all messages that belong to a facility in the same way, regardless of the source of the message (the Juniper Networks routing platform or the remote machine itself). For example, the following statements in the configuration of the routing platform called local-router direct messages from the authorization facility to the remote machine monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
 authorization info;
}
```

The default alternative facility for the local authorization facility is also authorization. If the syslogd utility on monitor is configured to write messages belonging to the authorization facility to the file /var/log/auth-attempts, the file contains both the messages generated when users log in to local-router and the messages generated when users log in to monitor. Although the name of the source machine appears in each system log message, the mixing of messages from multiple machines can make it more difficult to analyze the contents of the auth-attempts file.

To make it easier to separate the messages from each source, you can assign an alternative facility to all messages generated on local-router when they are directed to monitor. You can then configure the syslogd utility on monitor to write messages with the alternative facility to a different file from messages generated on monitor itself.

To change the facility used for all messages directed to a remote machine, include the facility-override statement at the [edit system syslog host *hostname*] hierarchy level:

```
[edit system syslog host hostname]
facility severity;
facility-override facility;
```

In general, it makes sense to specify an alternative facility that is not already in use on the remote machine, such as one of the localX facilities. On the remote machine, you must also configure the syslogd utility to handle the messages in the desired manner.

Table 12 on page 16 lists the facilities that you can specify in the facility-override statement.

Table 12: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts
daemon	Actions performed or errors encountered by system processes
ftp	Actions performed or errors encountered by the FTP process
kernel	Actions performed or errors encountered by the JUNOS kernel
local0	Local facility number 0
local1	Local facility number 1
local2	Local facility number 2
local3	Local facility number 3
local4	Local facility number 4
local5	Local facility number 5
local6	Local facility number 6
local7	Local facility number 7
user	Actions performed or errors encountered by user-space processes

We do not recommend including the facility-override statement at the [edit system syslog host other-routing-engine] hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its JUNOS system logging utility can interpret the JUNOS-specific names.

Examples: Assigning an Alternative Facility

Log all messages generated on the local routing platform at the error level or higher to the local0 facility on the remote machine called monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
 any error;
 facility-override local0;
}
```

Configure routing platforms located in and routing platforms located in New York to send messages to a single remote machine called central-logger.mycompany.com. The messages from California are assigned alternative facility local0 and the messages from New York are assigned to alternative facility local2.

- Configure California routing platforms to aggregate messages in the local0 facility:

```
[edit system syslog]
host central-logger.mycompany.com {
 change-log info;
 facility-override local0;
}
```

- Configure New York routing platforms to aggregate messages in the local2 facility:

```
[edit system syslog]
host central-logger.mycompany.com {
 change-log info;
 facility-override local2;
}
```

On central-logger, you can then configure the system logging utility to write messages from the local0 facility to the file california-config and the messages from the local2 facility to the file new-york-config.

Adding a Text String to System Log Messages

To add a text string to every system log message directed to a remote machine or to the other Routing Engine, include the log-prefix statement at the [edit system syslog host] hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
log-prefix string;
```

The string can contain any alphanumeric or special character except the equal sign (=) and the colon (:). It also cannot include the space character; do not enclose the string in quotation marks (“ “) in an attempt to include spaces in it.

The JUNOS system logging utility automatically appends a colon and a space to the specified string. The string is inserted after the identifier for the Routing Engine that generated the message.

Adding a String

Add the string M120 to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine hardware-logger.mycompany.com:

```
[edit system syslog]
host hardware-logger.mycompany.com {
 any info;
 log-prefix M120;
}
```

When these configuration statements are included on an M120 router called origin1, a message in the system log on hardware-logger.mycompany.com looks like the following:

```
Mar 9 17:33:23 origin1 M120: mgd[477]: UI_CMDLINE_READ_LINE: user 'root',
  command 'run show version'
```

Configuring the Size and Number of Log Files

To prevent log files from growing too large, the JUNOS system logging utility by default writes messages to a sequence of files of a defined size. The files in the sequence are referred to as *archive* files to distinguish them from the *active* file to which messages are currently being written. The default maximum size depends on the platform type:

- 128 kilobytes (KB) for J-series Services Routers
- 1 megabyte (MB) for M-series, MX-series, and T-series routing platforms
- 1 megabyte (MB) for M-series, MX-series, and T-series routing platforms

When an active log file called *logfile* reaches the maximum size, the logging utility closes the file, compresses it, and names the compressed archive file *logfile.0.gz*. The logging utility then opens and writes to a new active file called *logfile*. When the new *logfile* reaches the configured maximum size,*logfile.0.gz* is renamed *logfile.1.gz*, and the new *logfile* is closed, compressed, and renamed *logfile.0.gz*. By default, the logging utility creates up to 10 archive files in this manner. When the maximum number of archive files is reached, each time the active file reaches the maximum size the contents of the oldest archive file are lost (overwritten by the next oldest file). The logging utility by default also limits the users who can read log files to the root user and users who have the JUNOS maintenance permission.

You can include the archive statement to change the maximum size of each file, how many archive files are created, and who can read log files. To configure values that apply to all log files, include the archive statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
archive {
 files number;
 size size;
 (world-readable | no-world-readable);
}
```

To configure values that apply to a particular log file, include the archive statement at the [edit system syslog file *filename*] hierarchy level:

```
[edit system syslog file filename]
facility severity;
archive {
 files number;
 size size;
 (world-readable | no-world-readable);
}
```

files number specifies the number of files to create before the oldest file is overwritten. The value can be from **1** through **1000**.

size size specifies the maximum size of each file. The value can be from 64 KB (**64k**) through 1 gigabyte (**1g**); to represent megabytes, use the letter m after the integer. There is no space between the digits and the **k**, **m**, or **g** units letter.

world-readable enables all users to read log files. To restore the default permissions, include the **no-world-readable** statement.

Including Priority Information in System Log Messages

A message's facility and severity level are together referred to as its priority. By default, messages logged in the standard JUNOS format do not include information about priority. To include priority information in standard-format messages directed to a file, include the **explicit-priority** statement at the [**edit system syslog file** *filename*] hierarchy level:

```
[edit system syslog file filename]
facility severity;
explicit-priority;
```

NOTE: Messages logged in structured-data format include priority information by default (structured-data format is available in JUNOS Release 8.3 and later and for file destinations only). If you include the **structured-data** statement at the [**edit system syslog file** *filename*] hierarchy level along with the **explicit-priority** statement, the **explicit-priority** statement is ignored and messages are logged in structured-data format.

For information about the **structured-data** statement, see "Logging Messages in Structured-Data Format" on page 12. For information about the contents of a structured-data message, see "Displaying a Log File from a Single-Chassis System" on page 37.

To include priority information in messages directed to a remote machine or the other Routing Engine, include the **explicit-priority** statement at the [**edit system syslog host** (*hostname* | **other-routing-engine**)] hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
explicit-priority;
```

The priority recorded in a message always indicates the original, local facility name. If the **facility-override** statement is included for messages directed to a remote destination, the JUNOS system logging utility still uses the alternative facility for the messages themselves when directing them to the remote destination. For more information about alternative facilities, see "Changing the Alternative Facility Name for Remote Messages" on page 14.

When the **explicit-priority** statement is included, the JUNOS logging utility prepends codes for the facility name and severity level to the message tag name, if the message has one:

FACILITY-severity[-TAG]

(The tag is a unique identifier assigned to some JUNOS system log messages; for more information, see "Interpreting System Log Messages" on page 38 and "Displaying and Interpreting System Log Message Descriptions" on page 49.)

Table 13 on page 20 lists the facility codes that can appear in system log messages and maps them to facility names.

NOTE: If the second column in Table 13 on page 20 does not include the JUNOS facility name for a code, the facility cannot be included in a statement at the [edit system syslog] hierarchy level. The JUNOS software might use the facilities in Table 13 on page 20—and others that are not listed—when reporting on internal operations

Table 13: Facility Codes Reported in Priority Information

Code	JUNOS Facility Name	Type of Event or Error
AUTH	authorization	Authentication and authorization attempts
AUTHPRIV		Authentication and authorization attempts that can be viewed by superusers only
CHANGE	change-log	Changes to the JUNOS configuration
CONFLICT	conflict-log	Specified configuration is invalid on the routing platform type
CONSOLE		Messages written to /dev/console by the kernel console output driver
CRON		Actions performed or errors encountered by the cron process
DAEMON	daemon	Actions performed or errors encountered by system processes
DFC	dfc	Actions performed or errors encountered by the dynamic flow capture process
FIREWALL	firewall	Packet filtering actions performed by a firewall filter

Table 13: Facility Codes Reported in Priority Information *(continued)*

Code	JUNOS Facility Name	Type of Event or Error
FTP	ftp	Actions performed or errors encountered by the FTP process
INTERACT	interactive-commands	Commands issued at the JUNOS CLI prompt or invoked by a client application such as a JUNOScript or NETCONF client
KERN	kernel	Actions performed or errors encountered by the JUNOS kernel
NTP		Actions performed or errors encountered by the Network Time Protocol (NTP) process
PFE	pfe	Actions performed or errors encountered by the Packet Forwarding Engine
SYSLOG		Actions performed or errors encountered by the JUNOS system logging utility
USER	user	Actions performed or errors encountered by user-space processes

Table 14 on page 21 lists the numerical severity codes that can appear in system log messages and maps them to severity levels.

Table 14: Numerical Codes for Severity Levels Reported in Priority Information

Numerical Code	Severity Level	Description
0	emergency	System panic or other condition that causes the routing platform to stop functioning
1	alert	Conditions that require immediate correction, such as a corrupted system database
2	critical	Critical conditions, such as hard drive errors
3	error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels

Table 14: Numerical Codes for Severity Levels Reported in Priority Information *(continued)*

Numerical Code	Severity Level	Description
4	warning	Conditions that warrant monitoring
5	notice	Conditions that are not errors but might warrant special handling
6	info	Events or nonerror conditions of interest
7	debug	Software debugging messages (these appear only if a technical support representative has instructed you to configure this severity level)

In the following example, the CHASSISD_PARSE_COMPLETE message belongs to the daemon facility and is assigned severity info (6):

```
Aug 21 12:36:30 router1 chassisd[522]:

%DAEMON-6-CHASSISD_PARSE_COMPLETE: Using new configuration
```

When the explicit-priority statement is not included, the priority does not appear in the message:

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using
new configuration
```

For more information about message formatting, see “Displaying and Interpreting System Log Messages” on page 37.

Including the Year or Millisecond in Timestamps

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

```
Aug 21 12:36:30
```

To include the year, the millisecond, or both in the timestamp, include the time-format statement at the [edit system syslog] hierarchy level:

```
edit system syslog]
time-format (year | millisecond | year millisecond);
```

The modified timestamp is used in messages directed to each destination configured by a file, console, or user statement at the [edit system syslog] hierarchy level, but not to destinations configured by a host statement.

The following example illustrates the format for a timestamp that includes both the millisecond (401) and the year (2006):

```
Aug 21 12:36:30.401 2006
```

NOTE: Messages logged in structured-data format (available in JUNOS 8.3 and later for file destinations) include the year and millisecond by default. If you include the structured-data statement at the [edit system syslog file *filename*] hierarchy level along with the time-format statement, the time-format statement is ignored and messages are logged in structured-data format.

For information about the structured-data statement, see "Logging Messages in Structured-Data Format" on page 12. For information about the information in a structured-data message, see "Displaying a Log File from a Single-Chassis System" on page 37.

Using Regular Expressions to Refine the Set of Logged Messages

The predefined facilities group together related messages, but you can also use regular expression matching to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination.

To specify the text string that must (or must not) appear in a message for the message to be logged to a destination, include the match statement and specify the regular expression which the text string must match:

match "*regular-expression*";

You can include this statement at the following hierarchy levels:

- [edit system syslog file *filename*] (for a file)
- [edit system syslog user *(username* | ***)] (for the terminal session of one or all users)
- [edit system syslog host *(hostname* |other-routing-engine)] (for a remote destination)

In specifying the regular expression, use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions. Explaining regular expression syntax is beyond the scope of this document, but POSIX standards are available from the Institute of Electrical and Electronics Engineers (IEEE, http://www.ieee.org).

Table 15 on page 24 specifies which character or characters are matched by some of the regular expression operators that you can use in the match statement. In the

descriptions, the term term refers to either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.

NOTE: The match statement is not case-sensitive.

Table 15: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
| (pipe)	One of the terms that appear on either side of the pipe operator.
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is JUNOS software-specific.
^ (caret)	Start of a line, when the caret appears outside square brackets. One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
$ (dollar sign)	End of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number.
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

Using Regular Expressions

Filter messages that belong to the interactive-commands facility, directing those that include the string configure to the terminal of the root user:

```
[edit system syslog]
user root {
 interactive-commands any;
 match ".*configure.*";
}
```

Messages like the following appear on the root user's terminal when a user issues a configure command to enter configuration mode:

timestamp *router-name* mgd[PID]: UI_CMDLINE_READ_LINE: User *'user'*, command 'configure private'

Filter messages that belong to the daemon facility and have severity error or higher, directing them to the file /var/log/process-errors. Omit messages generated by the SNMP process (snmpd), instead directing them to the file /var/log/snmpd-errors:

```
[edit system syslog]
file process-errors {
 daemon error;
 match "!(.*snmpd.*)";
}
file snmpd-errors {
 daemon error;
 match ".*snmpd.*";
}
```

Disabling Logging of a Facility

To disable the logging of messages that belong to a particular facility, include the *facility* none statement in the configuration. This statement is useful when, for example, you want to log messages that have the same severity level and belong to all but a few facilities. Instead of including a statement for each facility you want to log, you can include the any severity statement and then a *facility* none statement for each facility that you do not want to log. For example, the following logs all messages at the error level or higher to the console, except for messages from the daemon and kernel facilities. Messages from those facilities are logged to the file /var/log/internals instead:

```
[edit system syslog]
console {
 any error;
 daemon none;
 kernel none;
}
file internals {
 daemon info;
 kernel info;
}
```

Examples: Configuring System Logging

Log messages about all commands entered by users at the CLI prompt or invoked by client applications such as JUNOScript or NETCONF clients, and all authentication or authorization attempts, both to the file cli-commands and to the terminal of any user who is logged in:

```
[edit system]
syslog {
 file cli-commands {
  interactive-commands info;
  authorization info;
 }
 user * {
  interactive-commands info;
  authorization info;
```

```
 }
}
```

Log all changes in the state of alarms to the file /var/log/alarms:

```
[edit system]
syslog {
 file alarms {
  kernel warning;
 }
}
```

Configure the handling of messages of various types, as described in the comments. Information is logged to two files, to the terminal of user alex, to a remote machine, and to the console:

```
[edit system]
syslog {
/* write all security-related messages to file /var/log/security */
 file security {
  authorization info;
  interactive-commands info;
 }
/* write messages about potential problems to file /var/log/messages: */
/* messages from “authorization” facility at level “notice” and above, */
/* messages from all other facilities at level “warning” and above */
 file messages {
  authorization notice;
  any warning;
 }
/* write all messages at level “critical” and above to terminal of user “alex” if */
/* that user is logged in */
 user alex {
  any critical;
 }
/* write all messages from the “daemon” facility at level “info” and above, and */
/* messages from all other facilities at level “warning” and above, to the */
/* machine monitor.mycompany.com */
 host monitor.mycompany.com {
  daemon info;
  any warning;
 }
/* write all messages at level “error” and above to the system console */
 console {
  any error;
 }
}
```

Configure the handling of messages generated when users issue JUNOS CLI commands, by specifying the interactive-commands facility at the following severity levels:

- info—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file /var/log/user-actions.

- notice—Logs a message when users issue the configuration mode commands rollback and commit. The example writes the messages to the terminal of user philip.
- warning—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

```
[edit system]
syslog {
 file user-actions {
  interactive-commands info;
 }
 user philip {
  interactive-commands notice;
 }
 console {
  interactive-commands warning;
 }
}
```

Configuring System Logging for a Routing Matrix

This section explains how to configure system logging for the T640 Internet routing nodes and TX Matrix platform in a routing matrix. It assumes you are familiar with system logging for single-chassis systems, as described in "Configuring System Logging for a Single-Chassis System" on page 7. For more information about routing matrixes, see the *JUNOS System Basics Configuration Guide* and the *TX Matrix Platform Hardware Guide*.

To configure system logging for all platforms in a routing matrix, include the syslog statement at the [edit system] hierarchy level on the TX Matrix platform. The syslog statement applies to every platform in the routing matrix.

```
[edit system]
syslog {
 archive {
  files number;
  size size;
  (world-readable | no-world-readable);
 }
 console {
 facility severity;
 }
 file filename {
 facility severity;
 explicit-priority;
 match "regular-expression";
 structured-data {
  brief;
 }
 archive {
  files number;
  size size;
  (world-readable | no-world-readable);
 }
}
host (hostname | other-routing-engine | scc-master) {
 facility severity;
 explicit-priority;
 facility-override facility;
 log-prefix string;
 match "regular-expression";
}
source-address source-address;
time-format (year | millisecond | year millisecond);
user (username | *) {
 facility severity ;
 match "regular-expression";
}
}
```

When included in the configuration on the TX Matrix platform, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every platform in the routing matrix:

- archive—Sets the size and number of log files archived on each platform in the routing matrix. See "Configuring the Size and Number of Log Files" on page 18.
- console—Directs the specified messages to the console of each platform in the routing matrix. See "Directing Messages to the Console" on page 13.
- file—Directs the specified messages to a file of the same name on each platform in the routing matrix. See "Directing Messages to a Log File" on page 11.
- match—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See "Using Regular Expressions to Refine the Set of Logged Messages" on page 23.

  The separate match statement at the [edit system syslog host scc-master] hierarchy level applies to messages forwarded from the T640 routing nodes to the TX Matrix platform. See "Configuring Optional Features for Forwarded Messages" on page 33.
- source-address—Sets the IP address of the routing platform to report in system log messages as the message source, when the messages are directed to the remote machines specified in all host *hostname* statements at the [edit system syslog] hierarchy level, for each platform in the routing matrix. The address is not reported in messages directed to the other Routing Engine on each platform or forwarded to the TX Matrix platform by the T640 routing nodes. See "Specifying an Alternative Source Address for System Log Messages" on page 14.
- structured-data—Writes messages to a file in structured-data format. See "Logging Messages in Structured-Data Format" on page 12.
- time-format—Adds the millisecond, year, or both to the timestamp in each standard-format message. See "Including the Year or Millisecond in Timestamps" on page 22.
- user—Directs the specified messages to the terminal session of one or more specified users on each platform in the routing matrix that they are logged in to. See "Directing Messages to a User Terminal" on page 12.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system. For more information, see the following sections:

- Configuring Message Forwarding in the Routing Matrix on page 29
- Configuring Optional Features for Forwarded Messages on page 33
- Directing Messages to a Remote Destination from the Routing Matrix on page 34
- Configuring System Logging Differently on Each Platform on page 35

Configuring Message Forwarding in the Routing Matrix

By default, the master Routing Engine on each T640 routing node forwards to the master Routing Engine on the TX Matrix platform all messages from all facilities with severity info and higher. To change the facility, the severity level, or both, include

the host scc-master statement at the [edit system syslog] hierarchy level on the TX Matrix platform:

```
[edit system syslog]
host scc-master {
 facility severity;
}
```

To disable message forwarding, set the facility to any and the severity level to none:

```
[edit system syslog]
host scc-master {
 any none;
}
```

In either case, the setting applies to all T640 routing nodes in the routing matrix.

To capture the messages forwarded by the T640 routing nodes (as well as messages generated on the TX Matrix platform itself), you must also configure system logging on the TX Matrix platform. Direct the messages to one or more destinations by including the appropriate statements at the [edit system syslog] hierarchy level on the TX Matrix platform:

- To a file, as described in "Directing Messages to a Log File" on page 11.
- To the terminal session of one or more specific users (or all users), as described in "Directing Messages to a User Terminal" on page 12.
- To the console, as described in "Directing Messages to the Console" on page 13.
- To a remote machine that is running the syslogd utility or to the other Routing Engine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix" on page 34.

As previously noted, the configuration statements included on the TX Matrix platform also configure the same destinations on each T640 routing node.

When specifying the severity level for local messages (at the [edit system syslog (file | host | console | user)] hierarchy level) and forwarded messages (at the [edit system syslog host scc-master] hierarchy level), you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the any facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

- Messages Logged When Local and Forwarded Severity Level Are the Same on page 30
- Messages Logged When Local Severity Level Is Lower on page 31
- Messages Logged When Local Severity Level Is Higher on page 32

Messages Logged When Local and Forwarded Severity Level Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix platform contains all messages from the logs on the T640 routing

nodes. For example, you can specify severity info for the /var/log/messages file, which is the default severity level for messages forwarded by T640 routing nodes:

```
[edit system syslog]
file messages {
 any info;
}
```

Table 16 on page 31 pecifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform

Table 16: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T640 routing node	Local	info
TX Matrix platform	Local	info
	Forwarded from T640 routing nodes	info

Messages Logged When Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix platform includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, you can specify severity notice for the /var/log/messages file and severity critical for forwarded messages

```
[edit system syslog]
file messages {
 any notice;
}
host scc-master {
 any critical;
}
```

Table 17 on page 32 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform. The T640 routing nodes forward only those messages with severity critical and higher, so the log on the TX Matrix platform does not include the messages with severity error, warning, or notice that the T640 routing nodes log locally:

Table 17: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T640 routing node	Local	notice
TX Matrix platform	Local	notice
	Forwarded from T640 routing nodes	critical

Messages Logged When Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix platform includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity critical for the /var/log/messages file and severity notice for forwarded messages:

```
[edit system syslog]
file messages {
 any critical;
}
host scc-master {
 any notice;
}
```

Table 18 on page 32 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform. Although the T640 routing nodes forward messages with severity notice and higher, the TX Matrix platform discards any of those messages with severity lower than critical (does not log forwarded messages with severity error, warning, or notice). None of the logs include messages with severity error or lower.

Table 18: Example: Local Severity Is critical, Forwarded Severity Is notice

Log Location	Source of Messages	Lowest Severity Included
T640 routing node	Local	critical
TX Matrix platform	Local	critical
	Forwarded from T640 routing nodes	critical

We do not recommend this type of configuration, because it wastes bandwidth for the routing nodes to forward messages that are not recorded in the log on the TX Matrix platform.

Configuring Optional Features for Forwarded Messages

To configure additional optional features when specifying how the T640 routing nodes forward messages to the TX Matrix platform, include statements at the [edit system syslog host scc-master] hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the explicit-priority statement. To insert a text string in each forwarded message, include the log-prefix statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the match statement.

```
[edit system syslog host scc-master]
  facility severity;
 explicit-priority;
 log-prefix string;
 match "regular-expression";
}
```

NOTE: You can also include the facility-override statement at the [edit system syslog host scc-master] hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the TX Matrix platform, because it runs the JUNOS system logging utility and can interpret the JUNOS-specific facilities. For more information about alternative facilities, see "Changing the Alternative Facility Name for Remote Messages" on page 14.

Including Priority Information in Forwarded Messages

When you include the explicit-priority statement at the [edit system syslog host scc-master] hierarchy level, messages forwarded to the TX Matrix platform include priority information. For the information to appear in a log file on the TX Matrix platform, you must also include the explicit-priority statement at the [edit system syslog file *filename*] hierarchy level for the file on the TX Matrix platform. As a consequence, the log file with the same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all platforms in the routing matrix, also include the explicit-priority statement at the [edit system syslog host *hostname*] hierarchy level for the remote machine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix" on page 34.

In the following example, the /var/log/messages file on all platforms includes priority information for messages with severity notice and higher from all facilities. The log

on the TX Matrix platform also includes messages with those characteristics forwarded from the T640 routing nodes.

```
[edit system syslog]
host scc-master {
 any notice;
 explicit-priority;
}
file messages {
 any notice;
 explicit-priority;
}
```

Adding a Text String to Forwarded Messages

When you include the log-prefix statement at the [edit system syslog host scc-master] hierarchy level, the string that you define appears in every message forwarded to the TX Matrix platform. For more information, see "Adding a Text String to System Log Messages" on page 17.

Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the match statement at the [edit system syslog host scc-master] hierarchy level, the regular expression that you specify controls which messages from the T640 routing nodes are forwarded to the TX Matrix platform. The regular expression is not applied to messages from the T640 routing notes that are directed to destinations other than the TX Matrix platform. For more information about regular expression matching, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 23.

Directing Messages to a Remote Destination from the Routing Matrix

You can configure a routing matrix to direct system logging messages to a remote machine or the other Routing Engine on each routing platform, just as on a single-chassis system. Include the host statement at the [edit system syslog] hierarchy level on the TX Matrix platform:

```
[edit system syslog]
host (hostname | other-routing-engine) {
 facility severity ;
 explicit-priority;
 facility-override facility;
 log-prefix string;
 match "regular-expression";
}
source-address source-address;
```

The TX Matrix platform directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (explicit-priority, facility-override, log-prefix, match, and source-address) also have the same effect as on a single-chassis system. For more information, see "Directing Messages to a Remote Machine or the Other Routing Engine" on page 13.

For the TX Matrix platform to include priority information when it directs messages that originated on a T640 routing node to the remote destination, you must also include the explicit-priority statement at the [edit system syslog host scc-master] hierarchy level.

The other-routing-engine statement does not interact with message forwarding from the T640 routing nodes to the TX Matrix platform. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (re0), the re0 Routing Engine on each T640 routing node sends messages to the re1 Routing Engine on its platform only. It does not also send messages directly to the re1 Routing Engine on the TX Matrix platform.

Because the configuration on the TX Matrix platform applies to the T640 routing nodes, any T640 routing node that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T640 routing nodes are configured to forward messages to the TX Matrix platform (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T640 routing node and the other from the TX Matrix platform. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see "Configuring Message Forwarding in the Routing Matrix" on page 29.
- If the source-address statement is configured at the [edit system syslog] hierarchy level, all platforms in the routing matrix report the same source routing platform in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single routing platform.
- If the log-prefix statement is included, the messages from all platforms in the routing matrix include the same text string. You cannot use the string to distinguish between the platforms in the routing matrix.

Configuring System Logging Differently on Each Platform

We recommend that all platforms in a routing matrix use the same configuration, which implies that you include system logging configuration statements on the TX Matrix platform only. In rare circumstances, however, you might choose to log different messages on different platforms. For example, if one platform in the routing matrix is experiencing problems with authentication, a Juniper Networks support representative might instruct you to log messages from the authorization facility on that platform.

To configure platforms separately, include configuration statements in the appropriate groups at the [edit groups] hierarchy level on the TX Matrix platform:

- To configure settings that apply to the TX Matrix platform but not the T640 routing nodes, include them in the re0 and re1 configuration groups.
- To configure settings that apply to particular T640 routing nodes, include them in the lccn-re0 and lccn-re1 configuration groups, where n is the line-card chassis (LCC) index number of the routing node.

When you use configuration groups, do not issue CLI configuration-mode commands to change the statements at the [edit system syslog] hierarchy level on the TX Matrix platform. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T640 routing nodes also. (We further recommend that you do not issue CLI configuration mode commands on the T640 routing nodes at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *JUNOS CLI User Guide*.

The following example shows how to configure the /var/log/messages files on three platforms to include different sets of messages:

- On the TX Matrix platform, local messages with severity info and higher from all facilities. The file does not include messages from the T640 routing nodes, because the host scc-master statement disables message forwarding.
- On the T640 routing node designated LCC0, messages from the authorization facility with severity info and higher.
- On the T640 routing node designated LCC1, messages with severity notice from all facilities.

```
[edit groups]
re0 {
 system {
  syslog {
   file messages {
    any info;
   }
   host scc-master {
    any none;
   }
  }
 }
}
re1 {
... same statements as for re0 ...
}
lcc0-re0 {
 system {
  syslog {
   file messages {
    authorization info;
   }
  }
 }
}
lcc0-re1 {
... same statements as for lcc0-re0 ...
}
lcc1-re0 {
 system {
  syslog {
   file messages {
    any notice;
```

```
    }
   }
  }
 }
 lcc0-re1 {
 ... same statements as for lcc1-re0 ...
 }
```

Displaying and Interpreting System Log Messages

This section explains how to display a log file and interpret the contents of system log messages:

For more information about the commands discussed in this section, see the *JUNOS System Basics and Services Command Reference.*

- Displaying a Log File from a Single-Chassis System on page 37
- Displaying a Log File from a Routing Matrix on page 37
- Interpreting System Log Messages on page 38
- Format of the message-source Field on page 45
- Examples: Displaying a Log File on page 48

Displaying a Log File from a Single-Chassis System

To display a log file stored on a single-chassis system, enter JUNOS CLI operational mode and issue either of the following commands:

```
user@host> show log log-filename
user@host> file show log-file-pathname
```

By default, the commands display the file stored on the local Routing Engine. To display the file stored on a particular Routing Engine, prefix the file- or pathname with the string re0 or re1 and a colon. The following examples both display the /var/log/messages file stored on the Routing Engine in slot 1:

```
user@host> show log re1:messages
user@host> file show re1:/var/log/messages
```

For information about the fields in a log message, see “Interpreting System Log Messages” on page 38. For examples, see “Examples: Displaying a Log File” on page 48.

Displaying a Log File from a Routing Matrix

One way to display a log file stored on the local Routing Engine of any of the individual platforms in a routing matrix (T640 routing nodes or TX Matrix platform) is to log in to a Routing Engine on the platform, enter JUNOS CLI operational mode, and issue the show log or file show command described in “Displaying a Log File from a Single-Chassis System” on page 37.

To display a log file stored on a T640 routing node during a terminal session on the TX Matrix platform, issue the show log or file show command and add a prefix that specifies the T640 routing node's LCC index number as lccn, followed by a colon. The index can be from 0 (zero) through 3:

user@host> **show log lcc***n:log-filename*
user@host> **file show lcc***n:log-file-pathname*

By default, the show log and file show commands display the specified log file stored on the master Routing Engine on the T640 routing node. To display the log from a particular Routing Engine, prefix the file- or pathname with the string lccn-master, lccn-re0, or lccn-re1, followed by a colon. The following examples all display the /var/log/messages file stored on the master Routing Engine (in slot 0) on routing node LCC2:

user@host> **show log lcc2:messages**
user@host> **show log lcc2-master:messages**
user@host> **show log lcc2-re0:messages**
user@host> **file show lcc2:/var/log/messages**

If the T640 routing nodes are forwarding messages to the TX Matrix platform (as in the default configuration), another way to view messages generated on a T640 routing node during a terminal session on the TX Matrix platform is simply to display a local log file. However, the messages are intermixed with messages from other T640 routing nodes and the TX Matrix platform itself. For more information about message forwarding, see "Configuring Message Forwarding in the Routing Matrix" on page 29.

For information about the fields in a log message, see "Interpreting System Log Messages" on page 38. For examples, see "Examples: Displaying a Log File" on page 48.

Interpreting System Log Messages

The fields in a message written to the system log depend on whether the message was generated by a JUNOS process or subroutine library, or by services on a PIC, and whether it is in standard format or structured-data format. For more information, see the following sections:

- Interpreting Messages Generated in Structured-Data Format on page 38
- Interpreting Messages Generated in Standard Format by a JUNOS Process or Library on page 43
- Interpreting Messages Generated in Standard Format by Services on a PIC on page 44

Interpreting Messages Generated in Structured-Data Format

Beginning in JUNOS Release 8.3, when the structured-data statement is included in the configuration for a log file, JUNOS processes and software libraries write messages to the file in structured-data format instead of the standard JUNOS format. For information about the structured-data statement, see "Logging Messages in Structured-Data Format" on page 12.

Structured-format makes it easier for automated applications to extract information from the message. In particular, the standardized format for reporting the value of variables (elements in the English-language message that vary depending on the circumstances that triggered the message) makes it easy for an application to extract those values. In standard format, the variables are interspersed in the message text and not identified as variables.

The structured-data format for a message includes the following fields (which appear here on two lines only for legibility):

<priority code>version timestamp hostname process processID TAG [junos@2636.platform variable-value-pairs] message-text

Table 19 on page 39 describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 19: Fields in Structured-Data Messages

Field	Description	Examples
<priority code>	Number that indicates the message's facility and severity. It is calculated by multiplying the facility number by 8 and then adding the numerical value of the severity. For a mapping of the numerical codes to facility and severity, see Table 20 on page 41.	<165> for a message from the pfe facility (facility=20) with severity notice (severity=5).
version	Version of the Internet Engineering Task Force (IETF) system logging protocol specification.	1 for the initial version
timestamp	Time when the message was generated, in one of two representations: ■ *YYYY-MM-DDTHH:MM:SS.MSZ* is the year, month, day, hour, minute, second and millisecond in Universal Coordinated Time (UTC) ■ *YYYY-MM-DDTHH:MM:SS.MS+/-HH:MM* is the year, month, day, hour, minute, second and millisecond in local time; the hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from UTC	2007-02-15T09:17:15.719Z is 9:17 AM UTC on 15 February 2007. 2007-02-15T01:17:15.719 -08:00 is the same timestamp expressed as Pacific Standard Time in the United States.
hostname	Name of the host that originally generated the message.	router1
process	Name of the JUNOS process that generated the message.	mgd
processID	UNIX process ID (PID) of the JUNOS process that generated the message.	3046

Table 19: Fields in Structured-Data Messages *(continued)*

Field	Description	Examples
TAG	JUNOS system log message tag, which uniquely identifies the message. For a list of the tags described in this reference, see "System Log Messages" on page 53.	UI_DBASE_LOGOUT_EVENT
junos@2636.platform	An identifier for the type of hardware platform that generated the message. The junos@2636 prefix indicates that the platform runs the JUNOS software. It is followed by a dot-separated numerical identifier for the platform type. For a list of the identifiers, see Table 21 on page 42.	junos@2636.1.1.1.2.18 for the M120 router
variable-value-pairs	A variable-value pair for each element in the *message-text* string that varies depending on the circumstances that triggered the message. Each pair appears in the format *variable="value"*.	username="regress"
message-text	English-language description of the event or error (omitted if the brief statement is included at the [edit system syslog file *filename* structured-data] hierarchy level). For the text for each message, see the chapters following "System Log Messages" on page 53.	User 'regress' exiting configuration mode

By default, the structured-data version of a message includes English text at the end, as in the following example (which appears on multiple lines only for legibility):

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
  [junos@2636.1.1.1.2.18 username="regress"] User 'regress' exiting configuration mode
```

When the brief statement is included at the [edit system syslog file *filename* structured-data] hierarchy level, the English text is omitted, as in this example:

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
  [junos@2636.1.1.1.2.18 username="regress"]
```

Table 20 on page 41 maps the codes that appear in the*priority-code* field to facility and severity level.

NOTE: Not all of the facilities and severities listed in Table 20 on page 41can be included in statements at the [edit system syslog] hierarchy level (some are used by internal processes). For a list of the facilities and severity levels that can be included in the configuration, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 9.

Table 20: Facility and Severity Codes in the priority-code Field

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
kernel (0)	1	1	2	3	4	5	6	7
user (1)	8	9	10	11	12	13	14	15
mail (2)	16	17	18	19	20	21	22	23
daemon (3)	24	25	26	27	28	29	30	31
authorization (4)	32	33	34	35	36	37	38	39
syslog (5)	40	41	42	43	44	45	46	47
printer (6)	48	49	50	51	52	53	54	55
news (7)	56	57	58	59	60	61	62	63
uucp (8)	64	65	66	67	68	69	70	71
clock (9)	72	73	74	75	76	77	78	79
authorization-private (10)	80	81	82	83	84	85	86	87
ftp (11)	88	89	90	91	92	93	94	95
ntp (12)	96	97	98	99	100	101	102	103
security (13)	104	105	106	107	108	109	110	111
console (14)	112	113	114	115	116	117	118	119
local0 (16)	128	129	130	131	132	133	134	135
dfc (17)	136	137	138	139	140	141	142	143
local2 (18)	144	145	146	147	148	149	150	151
firewall (19)	152	153	154	155	156	157	158	159
pfe (20)	160	161	162	163	164	165	166	167
conflict-log (21)	168	169	170	171	172	173	174	175
change-log (22)	176	177	178	179	180	181	182	183
interactive-commands (23)	184	185	186	187	188	189	190	191

Table 21 on page 42 lists the numerical identifiers for routing platforms that appear in the *platform* field. The identifier is derived from the platform's SNMP object identifier (OID) as defined in the Juniper Networks routing platform MIB. For more

information about OIDs, see the *JUNOS Network Management Configuration Guide*. For a downloadable version of the MIB, see http://www.juniper.net/techpubs/\software/junos/junosXX/swconfigXX-net-mgmt/html/mib-jnx-chas-defines.txt (replace *XX* with a release code such as 84 for JUNOS Release 8.4).

Table 21: Platform Identifiers in the platform Field

Identifier	Platform Name
1.1.1.2.1	M40 router
1.1.1.2.2	M20 router
1.1.1.2.3	M160 router
1.1.1.2.4	M10 router
1.1.1.2.5	M5 router
1.1.1.2.6	T640 routing node
1.1.1.2.7	T320 router
1.1.1.2.8	M40e router
1.1.1.2.9	M320 router
1.1.1.2.10	M7i router
1.1.1.2.11	M10i router
1.1.1.2.13	J2300 Services Router
1.1.1.2.14	J4300 Services Router
1.1.1.2.15	J6300 Services Router
1.1.1.2.17	TX Matrix platform
1.1.1.2.18	M120 router
1.1.1.2.19	J4350 Services Router
1.1.1.2.20	J6350 Services Router
1.1.1.2.23	J2320 Services Router
1.1.1.2.24	J2350 Services Router

Interpreting Messages Generated in Standard Format by a JUNOS Process or Library

The syntax of a standard-format message generated by a JUNOS software process or subroutine library depends on whether it includes priority information:

- When the explicit-priority statement is included at the [edit system syslog file *filename*] or [edit system syslog host (*hostname* | other-routing-engine)] hierarchy level, a system log message has the following syntax:

```
timestamp  message-source: %facility-severity-TAG: message-text
```

- When directed to the console or to users, or when the explicit-priority statement is not included for files or remote hosts, a system log message has the following syntax:

```
timestamp  message-source: TAG: message-text
```

Table 22 on page 43 describes the message fields.

Table 22: Fields in Standard-Format Messages Generated by a JUNOS Process or Library

Field	Description
timestamp	Time at which the message was logged.
message-source	Identifier of the process or component that generated the message and the routing platform on which the message was logged. This field includes two or more subfields, depending on how system logging is configured. See "Format of the message-source Field" on page 45.
facility	Code that specifies the facility to which the system log message belongs. For a mapping of codes to facility names, see Table 13 on page 20.
severity	Numerical code that represents the severity level assigned to the system log message. For a mapping of codes to severity names, see Table 14 on page 21.
TAG	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating software process or library. The entries in this reference are ordered alphabetically by this prefix. Not all processes on a routing platform use tags, so this field does not always appear. For a list of prefixes for the tags described in this reference, see "System Log Messages" on page 53.
message-text	Text of the message. For the text for each message, see the chapters following "System Log Messages" on page 53.

Interpreting Messages Generated in Standard Format by Services on a PIC

Standard-format system log messages generated by services on a PIC, such as the Adaptive Services (AS) PIC, have the following syntax:

```
timestamp  (FPC Slot fpc-slot, PIC Slot pic-slot) {service-set} [SERVICE]:
 optional-string TAG: message-text
```

NOTE: System logging for services on PICs is not configured at the [edit system syslog] hierarchy level as discussed in this chapter. For configuration information, see the *JUNOS Services Interfaces Configuration Guide*.

The (FPC Slot *fpc-slot* , PIC Slot *pic-slot*) field appears only when the standard system logging utility that runs on the Routing Engine writes the messages to the system log. When the PIC writes the message directly, the field does not appear.

Table 23 on page 44 describes the message fields.

Table 23: Fields in Messages Generated by a PIC

Field	Description
timestamp	Time at which the message was logged.
fpc-slot	Slot number of the Flexible PIC Concentrator (FPC) that houses the PIC that generated the message.
pic-slot	Number of the PIC slot on the FPC in which the PIC that generated the message resides.
service-set	Name of the service set that generated the message.
SERVICE	Code representing the service that generated the message. The codes include the following: ■ FWNAT—Network Address Translation (NAT) service ■ IDS—Intrusion detection service
optional-string	A text string that appears if the configuration for the PIC includes the log-prefix statement at the [edit interfaces interface-name services-options syslog] hierarchy level. For more information, see the *JUNOS Services Interfaces Configuration Guide*.
TAG	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating PIC. The entries in this reference are ordered alphabetically by this prefix.
message-text	Text of the message. For the text of each message, see “System Log Messages” on page 53.

Format of the message-source Field

The *message-source* field discussed in "Interpreting Messages Generated in Standard Format by a JUNOS Process or Library" on page 43 has two or more subfields, depending on whether the message is logged on a single-chassis system or on a platform in a routing matrix, and whether message forwarding is configured in the routing matrix.

For more information, see the following sections:

- The message-source Field on a Single-Chassis System on page 45
- The message-source Field on a TX Matrix Platform on page 45
- The message-source Field on a T640 Routing Node in a Routing Matrix on page 47

The message-source Field on a Single-Chassis System

The format of the *message-source* field in a message on a single-chassis system depends on whether the message was generated on the local Routing Engine or the other Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine appear only if its configuration includes the other-routing-engine statement at the [edit system syslog host] hierarchy level.

- When the local Routing Engine generated the message, there are two subfields:

```
hostname process[process-ID]
```

- When the other Routing Engine generated the message, there are three subfields:

```
hostname reX process[process-ID]
```

hostname is the hostname of the local Routing Engine.

process[process-ID] is the name and PID of the process that generated the message. If the re*X* field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [*process-ID*] part does not appear.

re*X* indicates that the other Routing Engine generated the message (*X* is 0 or 1).

The message-source Field on a TX Matrix Platform

The format of the *message-source* field in a message on a TX Matrix platform depends on several factors:

- Whether the message was generated on the TX Matrix platform or a T640 routing node in the routing matrix. By default, the master Routing Engine on each T640 routing node forwards messages from all facilities with severity info and higher to the master Routing Engine on the TX Matrix platform. When you configure system logging on the TX Matrix platform, its logs include the forwarded messages. For more information, see "Configuring Message Forwarding in the Routing Matrix" on page 29.

- Whether the message was generated on the local Routing Engine or the other Routing Engine on the originating machine (TX Matrix platform or T640 routing node). Messages from the other Routing Engine appear only if its configuration includes the other-routing-engine statement at the [edit system syslog host] hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 24 on page 46 specifies the format of the message-source field in the various cases.

Table 24: Format of message-source Field in Messages Logged on TX Matrix Platform

Generating Machine	Generating Routing Engine	Process or Component	Format
TX Matrix platform	Local	Process	*hostname process[processID]*
		Component	*hostname scc-reX process[processID]*
	Other	Process	*hostname scc-reX scc-componentZ process*
		Component	*hostname scc-reX scc-componentZ process*
T640 routing node	Local	Process	*hostname lccY-masterprocess[processID]*
		Component	*hostname lccY-master scc-componentZ process*
	Other	Process	*hostname lccY-master lccY-reX process[processID]*
		Component	*hostname lccY-master lccY-reX lccY-componentZ process*

hostname is the hostname of the local Routing Engine on the TX Matrix platform.

lccY-master is the master Routing Engine on the T640 routing node with the indicated LCC index number (*Y* is from 0 through 3).

lccY-reX indicates that the backup Routing Engine on the T640 routing node generated the message (*X* is 0 or 1). The routing node has the indicated LCC index number (*Y* matches the value in the lccY-master field.

lccY-componentZ process identifies the hardware component and process on the T640 routing node that generated the message (*Y* matches the value in the lccY-master field and the range of values for *Z* depends on the component type). For example, lcc2-fpc1 PFEMAN refers to a process on the FPC in slot 1 on the T640 routing node with index LCC2.

process[process-ID] is the name and PID of the kernel or user-space process that generated the message. If the scc-reX or lccY-reX field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [*process-ID*] part does not appear.

scc-componentZ process identifies the hardware component and process on the TX Matrix platform that generated the message (the range of values for *Z* depends on the component type). For example, spmb1 GSIB refers to a process on one of the processor boards in the Switch Interface Board (SIB) with index 1.

scc-reX indicates that the other Routing Engine on the TX Matrix platform generated the message (*X* is 0 or 1).

The message-source Field on a T640 Routing Node in a Routing Matrix

The format of the *message-source* field in a message on a T640 routing node in a routing matrix depends on two factors:

- Whether the message was generated on the local Routing Engine or the other Routing Engine. Messages from the other Routing Engine appear only if its configuration includes the other-routing-engine statement at the [edit system syslog host] hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 25 on page 47 specifies the format of the *message-source* field in the various cases.

Table 25: Format of message-source Field in Messages Logged on TX Matrix Platform

Generating Routing Engine	Process or Component	Format
Local	Process	*hostname-lccY process[processID]*
	Component	*hostname-lccY lccY-componentZ process*
Other	Process	*hostname-lccY lccY-reX process[processID]*
	Component	*hostname-lccY lccY-reX lccY-componentZ process*

hostname-lccY is the hostname of the local Routing Engine and the T640 routing node's LCC index number.

lccY-componentZ process identifies the hardware component and process that generated the message (*Y* matches the value in the *hostname-lccY* field and the range of values for *Z* depends on the component type). For example, lcc0-fpc0 CMLC refers to a process on the FPC in slot 0. The T640 routing node has index LCC0 in the routing matrix.

lccY-reX indicates that the other Routing Engine on the routing node generated the message (Y matches the value in the *hostname-lccY* field and *X* is 0 or 1).

process[process-ID] is the name and PID of the kernel or user-space process that generated the message. If the *lccY-reX* field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [*process-ID*] part does not appear.

Examples: Displaying a Log File

Display the contents of the /var/log/messages file stored on the local Routing Engine. (The /var/log directory is the default location for log files, so you do not need to include it in the filename. The messages file is a commonly configured destination for system log messages.)

```
user@host> show log messages Apr 11 10:27:25 router1 mgd[3606]:
   UI_DBASE_LOGIN_EVENT: User 'barbara' entering configuration mode
Apr 11 10:32:22 router1 mgd[3606]: UI_DBASE_LOGOUT_EVENT: User 'barbara'
   exiting configuration mode
Apr 11 11:36:15 router1 mgd[3606]: UI_COMMIT: User 'root' performed commit: no
   comment
Apr 11 11:46:37 router1 mib2d[2905]: SNMP_TRAP_LINK_DOWN: ifIndex 82,
   ifAdminStatus up(1), ifOperStatus down(2), ifName at-1/0/0
```

Display the contents of the file /var/log/processes, which has been previously configured to include messages from the daemon facility. When issuing the file show command, you must specify the full pathname of the file:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
   SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
Feb 22 20:35:07 router1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
   trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 router1 snmpd[359]: SNMPD_TRAP_WARM_START:
   trap_generate_warm: SNMP trap: warm start
Feb 23 07:38:19 router1 snmpd[359]: SNMPD_TRAP_COLD_START:
   trap_generate_cold: SNMP trap: cold start
```

Display the contents of the file /var/log/processes when the explicit-priority statement is included at the [edit system syslog file processes] hierarchy level:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
   start
Feb 22 20:35:07 router1 snmpd[359]:
%DAEMON-6-SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler: cleared
   all throttled traps
Feb 23 07:34:56 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
   start
Feb 23 07:38:19 router1 snmpd[359]:
%DAEMON-2-SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold start
```

Getting Help About System Log Messages

System log message tag names begin with a prefix that indicates which JUNOS software process, subroutine library, or service on a PIC generated the message. This section explains how to learn more about the messages with each prefix, both in this reference and while you are using the CLI.

For a list of the prefixes for messages described in this reference, see "System Log Messages" on page 53. For information about displaying and interpreting messages, see the following sections:

- Displaying and Interpreting System Log Message Descriptions on page 49
- Examples: Displaying System Log Message Descriptions on page 51

Displaying and Interpreting System Log Message Descriptions

This reference lists the messages available at the time of its publication. To display the list of messages that applies to the version of the JUNOS software that is running on a routing platform, enter JUNOS CLI operational mode and issue the following command:

user@host> **help syslog ?**

To display the list of available descriptions for tags whose names begin with a specific character string, substitute the string (in all capital letters) for the variable *TAG-PREFIX* (there is no space between the prefix and the question mark):

user@host> **help syslog** *TAG-PREFIX***?**

To display the complete descriptions for tags whose name includes a regular expression, substitute the expression for the variable regex. The match is not case-sensitive.

user@host> **help syslog** *regex*

To display the complete description of a particular message, substitute its name for the variable *TAG* (in all capital letters):

user@host> **help syslog** *TAG*

Table 26 on page 49 describes the fields in a system log message description in this reference or in the CLI.

Table 26: Fields in System Log Message Descriptions

Field Name in Reference	Field Name in CLI	Description
—	Name	The message tag in all capital letters.

Table 26: Fields in System Log Message Descriptions *(continued)*

Field Name in Reference	Field Name in CLI	Description
System Log Message	Message	Text of the message written to the system log. In the log, a specific value is substituted for each variable that appears in italics in this reference or in angle brackets (< >) in the CLI. In this reference, the message text appears on the second line of the System Log Message field. The first line is the message tag (the same text as in the CLI Name field). The prefix on each tag identifies the message source and the rest of the tag indicates the specific event or error. "System Log Messages" on page 53 lists the prefixes for which this reference includes entries.
—	Help	Short description of the message, which also appears in the right-hand column of CLI output for the help syslog command when the output lists multiple messages.
Description	Description	More detailed explanation of the message.
Type	Type	Category to which the message belongs: ■ Error: The message reports an error or failure condition that might require corrective action. ■ Event: The message reports a condition or occurrence that does not generally require corrective action.
Severity	Severity	Message severity level as described in Table 10 on page 10.
Cause	Cause	(Optional) Possible cause for message generation. There can be more than one cause.

Table 26: Fields in System Log Message Descriptions *(continued)*

Field Name in Reference	Field Name in CLI	Description
Action	Action	(Optional) Action you can perform to resolve the error or failure condition described in the message. If this field does not appear in an entry, either no action is required or the action is self-explanatory.

Examples: Displaying System Log Message Descriptions

Display the list of all currently available system log message descriptions:

user@host> **help syslog ?**

```
Possible completions:
<syslog-tag>   Syslog tag
 . . .      . . .
BOOTPD_ARG_ERR   Command-line option was invalid
BOOTPD_BAD_ID   Request failed because assembly ID was unknown
BOOTPD_BOOTSTRING  tnp.bootpd provided boot string
BOOTPD_CONFIG_ERR  tnp.bootpd could not parse configuration file;
       used default settings
BOOTPD_CONF_OPEN  tnp.bootpd could not open configuration file
BOOTPD_DUP_REV   Extra boot string definitions for revision were
       ignored
---(more 4%)---
```

Display the list of all currently available system log message descriptions for tags that begin with the letters ACCT (there is no space between ACCT and the question mark, and some descriptions are shortened for legibility):

user@host> **help syslog ACCT?**

```
Possible completions:
<syslog-tag>       System log tag or regular expression
ACCT_ACCOUNTING_FERROR    Error occurred during file processing
ACCT_ACCOUNTING_FOPEN_ERROR   Open operation failed on file
ACCT_ACCOUNTING_SMALL_FILE_SIZE Maximum file size is smaller than ...
ACCT_BAD_RECORD_FORMAT    Record format does not match accounting profile
ACCT_CU_RTSLIB_ERROR    Error occurred obtaining current class usage ...
ACCT_FORK_ERR       Could not create child process
ACCT_FORK_LIMIT_EXCEEDED   Could not create child process because of limit
ACCT_GETHOSTNAME_ERROR    gethostname function failed
ACCT_MALLOC_FAILURE     Memory allocation failed
ACCT_UNDEFINED_COUNTER_NAME  Filter profile used undefined counter name
ACCT_XFER_FAILED      Attempt to transfer file failed
ACCT_XFER_POPEN_FAIL    File transfer failed
```

Display the description of the UI_CMDLINE_READ_LINE message:

user@host> **help syslog UI_CMDLINE_READ_LINE**

```
Name:    UI_CMDLINE_READ_LINE
Message:   User '<users>', command '<input>'
Help:    User entered command at CLI prompt
Description: The indicated user typed the indicated command at the CLI
     prompt and pressed the Enter key, sending the command string
     to the management process (mgd).
Type:    Event: This message reports an event, not an error
Severity:   info
```

Part 2
System Log Messages

Chapter 2

ACCT System Log Messages

This chapter describes messages with the ACCT prefix. They are generated by the accounting statistics process, which collects and records interface, filter, and class usage statistics.

ACCT_ACCOUNTING_FERROR

System Log Message Unexpected error *error-code* from file *filename*

Description An error prevented the accounting statistics process from processing the indicated file.

Type Error: An error occurred

Severity warning

ACCT_ACCOUNTING_FOPEN_ERROR

System Log Message Failed to open file *filename*: *error-code*

Description The accounting statistics process could not open the indicated file.

Type Error: An error occurred

Severity warning

ACCT_ACCOUNTING_SMALL_FILE_SIZE

System Log Message File *filename* size (*file-size*) is smaller than record size (*record-size*)

Description The size limit configured for the indicated file is smaller than the record to be written to it.

Type Error: An error occurred

Severity warning

ACCT_BAD_RECORD_FORMAT

System Log Message Invalid statistics record: *entry*

Description The number of columns in the indicated record does not match the number of columns in the accounting profile.

Type Error: An error occurred

Severity warning

ACCT_CU_RTSLIB_ERROR

System Log Message Error getting class usage statistics for interface *interface-name.unit-id*: *error-message*

Description The accounting statistics process could not obtain current class usage statistics.

Type Error: An error occurred

Severity error

ACCT_FORK_ERR

System Log Message Unable to fork: *error-message*

Description The accounting statistics process could not create a child process for transferring files, for the indicated reason.

Type Error: An error occurred

Severity error

ACCT_FORK_LIMIT_EXCEEDED

System Log Message Unable to fork: too many child processes

Description The accounting statistics process could not create a child process for transferring files, because adding another child would have made the number of children exceed the limit.

Type Error: An error occurred

Severity error

ACCT_GETHOSTNAME_ERROR

System Log Message Error *error-code* trying to get hostname

Description A call to the gethostname() function failed.

Type Error: An error occurred

Severity error

ACCT_MALLOC_FAILURE

System Log Message Memory allocation failed while reallocating filter profile interface list

Description The accounting statistics process could not allocate memory from the heap.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

ACCT_UNDEFINED_COUNTER_NAME

System Log Message Counter *profile-name* in accounting profile *counter-name* is not defined in a firewall using this filter profile

Description The indicated filter profile referenced the indicated counter name, which is not defined in a firewall filter that uses the filter profile.

Type Error: An error occurred

Severity warning

Action Change the filter profile counter name to match the name defined in the firewall configuration.

ACCT_XFER_FAILED

System Log Message Error transferring *filename*

Description An attempt to transfer the indicated file failed.

Type Error: An error occurred

Severity error

ACCT_XFER_POPEN_FAIL

System Log Message Error *error-code* in invoking command *command* to transfer file *filename*

Description A call to the popen() function failed when the accounting statistics process invoked the indicated command to transfer the indicated file.

Type Error: An error occurred

Severity error

Chapter 3

ANCPD System Log Messages

This chapter describes messages with the ANCPD prefix. They are generated by the access node control protocol process (ancpd), also known as layer 2 control (l2c), which works with a special internet group management protocol (igmp) session to collect outgoing interface (oif) mapping events in a scalable manner.

ANCPD_COMMAND_OPTIONS

System Log Message ancpd_cmd_opts called with option *index* arg *argument*

Description The access node control protocol process (ancpd) command line options were not handled by junos_app_init.

Type Event: This message reports an event, not an error

Severity info

Chapter 4

ANTISPAM System Log Messages

This chapter describes messages with the ANTISPAM prefix. They are generated by the antispam process, which decides what action should be performed when the device detects a message that it deems to be spam.

ANTISPAM_SPAM_DETECTED

System Log Message AntiSpam: SPAM detected: *source-name* (*source-address*) *action* reason: *reason*

Description The email is detected as a spam; the IP address of the source and its name will be logged together with the reason for it being categorized as spam

Type Event: This message reports an event, not an error

Severity info

Cause The email is detected as a spam

Action Verify the spam to make sure it is not a false positive

ANTISPAM_SPAM_DETECTED_MT

System Log Message AntiSpam: SPAM detected: *source-name* (*source-address*) *action* reason: *reason*

Description The email is detected as a spam; the IP address of the source and its name will be logged together with the reason for it being categorized as spam

Type Event: This message reports an event, not an error

Severity info

Cause The email is detected as a spam

Action Verify the spam to make sure it is not a false positive

Chapter 5

APPIDD System Log Messages

This chapter describes messages with the APPIDD prefix. They are generated by application identification process (appid), which is a passive application protocol identification library that implements a state machine for efficient pattern matching of regex-like application content signatures.

APPIDD_SCHEDULED_UPDATE_FAILED

System Log Message Failed to update application packge. error: *error-message*

Description The scheduled application-identification application package update failed to start. Device will try it again at the next scheduled time

Type Error: An error occurred

Severity error

Chapter 6

APPPXY System Log Messages

This chapter describes messages with the APPXY prefix. They are generated by the application proxy process (appxy).

APPPXY_RESOURCE_OVERUSED

System Log Message ApplicationProxy: Suspicious client *source-address*:*source-port* (-> *destination-address*:*destination-port*) used *percentage-value* connections, which exceeded the maximum allowed *maximum-value* connections

Description For ApplicationProxy, the amount of traffic from the specified source address exceeded the amount permitted from one source. The maximum amount of traffic from one source is a fixed percentage of the total amount of traffic.

Type Event: This message reports an event, not an error

Severity error

APPPXY_RESOURCE_OVERUSED_MT

System Log Message ApplicationProxy: Suspicious client *source-address*:*source-port* (-> *destination-address*:*destination-port*) used *percentage-value* connections, which exceeded the maximum allowed *maximum-value* connections

Description For ApplicationProxy, the amount of traffic from the specified source address exceeded the amount permitted from one source. The maximum amount of traffic from one source is a fixed percentage of the total amount of traffic

Type Event: This message reports an event, not an error

Severity error

APPPXY_SESSION_ABORT

System Log Message ApplicationProxy: session from *source-address*:*source-port* to *destination-address*:*destination-port* aborted due to *error-message* (code *error-code*)

Description Report application protocol (ftp/http/pop3/smtp/imap) session is aborted

Type Event: This message reports an event, not an error

Severity warning

APPPXY_SESSION_ABORT_MT

System Log Message ApplicationProxy: session from *source-address*:*source-port* to *destination-address*:*destination-port* aborted due to *error-message* (code *error-code*)

Description Report application protocol (ftp/http/pop3/smtp/imap) session is aborted

Type Event: This message reports an event, not an error

Severity warning

Chapter 7

ASP System Log Messages

This chapter describes messages with the ASP prefix. They are generated by services on the Adaptive Services Physical Interface Card (AS PIC), such as stateful firewall, Network Address Translation (NAT), and intrusion detection service (IDS). For information about configuring system logging for services on the AS PIC, see the *JUNOS Services Interfaces Configuration Guide*.

For information about the fields in messages with the ASP prefix, see "Interpreting Messages Generated in Standard Format by Services on a PIC" on page 43.

ASP_COS_RULE_MATCH

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type* rule-set: *rule-set-name*, rule: *rule-name*, term: *term-name*

Description A packet matched the indicated term in the indicated class-of-service (CoS) rule. If the rule belongs to a rule set, the name of the rule set is also displayed. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity info

ASP_IDS_HOST_RATE

System Log Message Host *destination-address*, *event-type* ... rate = *rate* events/sec

Description The indicated event occurred at the indicated rate (events per second) for the indicated destination IP address. The rate exceeds the intrusion detection services (IDS) threshold configured with the 'threshold' statement at the [edit services rule < rule-name > term < term-name > then logging] hierarchy level. This message is logged every 60 seconds until the rate no longer exceeds the threshold.

Type Event: This message reports an event, not an error

Severity error

ASP_IDS_HOST_RATE_APP

System Log Message Host *destination-address* (*application*), *event-type* ... rate = *rate* events/sec

Description The indicated event occurred at the indicated rate (events per second) for the indicated application at the indicated destination IP address. The rate exceeds the intrusion detection services (IDS) threshold set by the 'threshold' statement at the [edit services ids rule <rule-name> term <term-name> then logging] hierarchy level. The application is specified by the 'applications' or 'application-sets' statement at the [edit services ids rule <rule-name> term <term-name> from] hierarchy level. This message is logged every 60 seconds until the rate no longer exceeds the threshold.

Type Event: This message reports an event, not an error

Severity error

ASP_IDS_INV_CLEAR_QUERY

System Log Message CLEAR: Invalid query type *received-value* expecting *expected-value*

Description Intrusion detection services (IDS) received a request to clear information from IDS tables. The request included the indicated type of query, which IDS cannot interpret.

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

ASP_IDS_INV_CLEAR_QUERY_VER

System Log Message CLEAR: Invalid query version *received-value* expecting *expected-value*

Description Intrusion detection services (IDS) received a request to clear information from IDS tables. The request's version number did not match the version number of requests that IDS can service.

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

ASP_IDS_INV_SHOW_QUERY

System Log Message SHOW: Invalid query type *received-value* expecting *expected-value*

Description Intrusion detection services (IDS) received a request to show information from IDS tables. The request included the indicated type of query, which IDS cannot interpret.

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

ASP_IDS_INV_SHOW_QUERY_VER

System Log Message SHOW: Invalid query version *received-value* expecting *expected-value*

Description Intrusion detection services (IDS) received a request to show information from IDS tables. The request's version number did not match the version number of requests that IDS can service.

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

ASP_IDS_LIMIT_FLOW_RATE_BY_DEST

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and did not create a new flow, because the flow rate at the firewall exceeded the intrusion detection services (IDS) limit configured by the 'rate' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-destination] hierarchy level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_FLOW_RATE_BY_PAIR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and did not create a new flow, because the flow rate at the firewall exceeded the intrusion detection services (IDS) limit configured by the 'rate' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-pair] hierarchy level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_FLOW_RATE_BY_SRC

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and did not create a new flow, because the flow rate at the firewall exceeded the intrusion detection services (IDS) limit configured by the 'rate' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-source] hierarchy

level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_OPEN_FLOWS_BY_DEST

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and did not create a new flow, because the number of open flows exceeded the intrusion detection services (IDS) limit configured by the 'maximum' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-destination] hierarchy level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_OPEN_FLOWS_BY_PAIR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and did not create a new flow, because the number of open flows exceeded the intrusion detection services (IDS) limit configured by the 'maximum' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-pair] hierarchy level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_OPEN_FLOWS_BY_SRC

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and did not create a new flow, because the number of open flows exceeded the intrusion detection services (IDS) limit configured by the 'maximum' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-source] hierarchy level. The discarded packet contained the indicated information about its

protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_PKT_RATE_BY_DEST

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the number of packets per second (aggregated over all monitored flows) exceeded the intrusion detection services (IDS) limit configured by the 'packets' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-destination] hierarchy level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_PKT_RATE_BY_PAIR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the number of packets per second (aggregated over all monitored flows) exceeded the intrusion detection services (IDS) limit configured by the 'packets' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-pair] hierarchy level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_LIMIT_PKT_RATE_BY_SRC

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the number of packets per second (aggregated over all monitored flows) exceeded the intrusion detection services (IDS) limit configured by the 'packets' statement at the [edit services ids rule < rule-name > term < term-name > then session-limit by-source] hierarchy level. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_IDS_NO_MEM_SHOW_CMD

System Log Message Not enough memory for show command

Description Intrusion detection services (IDS) could not service a request to show information from IDS tables, because not enough memory was available.

Type Error: An error occurred

Severity critical

ASP_IDS_NULL_CLEAR_QUERY

System Log Message Failure: NULL query for CLEAR command.

Description Intrusion detection services (IDS) invoked a query handler to service a request to clear information from IDS tables. The handler did not receive the request.

Type Event: This message reports an event, not an error

Severity critical

Action Contact your technical support representative.

ASP_IDS_NULL_SHOW_QUERY

System Log Message Failure: NULL query for SHOW command.

Description Intrusion detection services (IDS) invoked a query handler to service a request to show information from IDS tables. The handler did not receive the request.

Type Event: This message reports an event, not an error

Severity critical

Action Contact your technical support representative.

ASP_IDS_RULE_MATCH

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type* rule-set: *rule-set-name*, rule: *rule-name*, term: *term-name*

Description A packet matched the indicated term in the indicated intrusion detection services (IDS) rule. If the rule belongs to a rule set, the rule set name is also displayed. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity info

ASP_IDS_SYN_COOKIE_OFF

System Log Message Host *destination-address*, SYN-COOKIE protection deactivated

Description Intrusion detection services (IDS) deactivated SYN cookie protection for the indicated destination address. IDS deactivates this protection when it learns from the stateful firewall that the rate of certain events has returned to a level below the threshold set by the 'threshold' statement at the [edit services ids rule <rule-name> term <term-name> then syn-cookie] hierarchy level. The relevant events include the ones reported by the ASP_IDS_TCP_SYN_ATTACK, ASP_SFW_SYN_DEFENSE, and ASP_SFW_TCP_SCAN system log messages.

Type Event: This message reports an event, not an error

Severity error

ASP_IDS_SYN_COOKIE_ON

System Log Message Host *destination-address*, SYN-COOKIE protection activated

Description Intrusion detection services (IDS) activated SYN cookie protection for the indicated destination address, because it learned from the stateful firewall that the rate of certain events exceeded the threshold set by the 'threshold' statement at the [edit services ids rule <rule-name> term <term-name> then syn-cookie] hierarchy level. The events include the ones reported by the ASP_IDS_TCP_SYN_ATTACK, ASP_SFW_SYN_DEFENSE, and ASP_SFW_TCP_SCAN system log messages. When SYN cookie protection is activated for a flow to a destination and the TCP handshake has not completed, the stateful firewall generates a SYN/ACK packet for each SYN packet directed to the destination.

Type Event: This message reports an event, not an error

Severity error

ASP_IDS_TCP_SYN_ATTACK

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall received the packet with the indicated characteristics and determined that it was a duplicate Transmission Control Protocol (TCP) SYN packet (the SYN flag was set and a SYN packet was already received for the flow to the destination). The event was reported to intrusion detection services (IDS) and can cause IDS to activate SYN cookie protection. The packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity error

ASP_L2TP_MESSAGE_INCOMPLETE

System Log Message IPC message lacked variable portion

Description The Layer 2 Tunneling Protocol (L2TP) did not process an interprocess communication (IPC) message because the variable portion of the message was missing.

Type Error: An error occurred

Severity error

ASP_L2TP_NO_MEM

System Log Message Unable to allocate memory for L2TP flow for tunnel *tunnel-id*, session *session-id*

Description The Layer 2 Tunneling Protocol (L2TP) could not allocate the memory it needed to create a flow for the indicated tunnel and session.

Type Error: An error occurred

Severity error

ASP_L2TP_OBJ_CAC_FAIL

System Log Message Unable to allocate object-cache memory for flow (unit *unit-id*, tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol (L2TP) could not allocate memory from an object cache for the flow defined by the indicated unit, tunnel, and session.

Type Error: An error occurred

Severity error

ASP_L2TP_STATS_BULK_QUERY_FAILED

System Log Message Number of queries (*num-queries*) in statistics request exceeded limit (*max-queries*)

Description The Layer 2 Tunneling Protocol (L2TP) did not process an interprocess communication (IPC) request for statistics because it included the indicated the number of queries, which exceeds the limit as indicated.

Type Error: An error occurred

Severity error

ASP_L2TP_STATS_VERSION_INVALID

System Log Message Invalid version *received-value* on statistics request (expected *expected-value*)

Description The Layer 2 Tunneling Protocol process (l2tpd) received a request for statistics with the indicated version, which is not the indicated, supported version.

Type Error: An error occurred

Severity error

ASP_L2TP_TUN_GRP_ADD_FAIL_ALLOC

System Log Message Unable to add tunnel group for service set *service-set*: could not allocate ID

Description The Layer 2 Tunneling Protocol (L2TP) could not add a tunnel group for the indicated service set because it could not allocate an internal ID.

Type Error: An error occurred

Severity error

ASP_L2TP_TUN_GRP_ADD_FAIL_EXISTS

System Log Message Unable to add tunnel group *group-id*: it already exists

Description The Layer 2 Tunneling Protocol (L2TP) could not add a tunnel group with the indicated ID because it already existed.

Type Error: An error occurred

Severity error

ASP_L2TP_TUN_GRP_CHG_FAIL_ALLOC

System Log Message Unable to change tunnel group for service set *service-set*: could not allocate ID

Description The Layer 2 Tunneling Protocol (L2TP) could not change a tunnel group for the indicated service set because it could not allocate an internal ID.

Type Error: An error occurred

Severity error

ASP_L2TP_TUN_GRP_CHG_FAIL_INVLD

System Log Message Unable to change tunnel group *group-id*: ID is invalid

Description The Layer 2 Tunneling Protocol (L2TP) could not change the tunnel group with the indicated internal ID, because the ID is invalid.

Type Error: An error occurred

Severity error

ASP_L2TP_TUN_GRP_DEL_FAIL_INVLD

System Log Message Unable to delete tunnel group *group-id*: ID is invalid

Description The Layer 2 Tunneling Protocol (L2TP) could not delete the tunnel group with the indicated internal ID, because the ID is invalid.

Type Error: An error occurred

Severity error

ASP_NAT_OUTOF_ADDRESSES

System Log Message natpool *nat-pool-name* is out of addresses

Description Network Address Translation (NAT) services could not allocate an address from the indicated NAT pool, because no addresses were available.

Type Event: This message reports an event, not an error

Severity warning

ASP_NAT_OUTOF_PORTS

System Log Message natpool *nat-pool-name* is out of ports

Description Network Address Translation (NAT) services could not allocate a port from the indicated NAT pool, because no ports were available.

Type Event: This message reports an event, not an error

Severity warning

ASP_NAT_POOL_RELEASE

System Log Message natpool release *address*:*port*[*count*]

Description Network Address Translation (NAT) services made the indicated number of ports available in the pool for the indicated address, starting at the indicated port number.

Type Event: This message reports an event, not an error

Severity info

ASP_NAT_RULE_MATCH

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type* rule-set: *rule-set-name*, rule: *rule-name*, term: *term-name*

Description A packet matched the indicated term in the indicated Network Address Translation (NAT) rule. If the rule belongs to a rule set, the rule set name is also displayed. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity info

ASP_PGCP_IPC_MSG_WRITE_FAILED

System Log Message Unable to write IPC message (type *message-type*, subtype *message-subtype*): status code *status*

Description The Packet Gateway Control Protocol (PGCP) client on the MultiServices Physical Interface Card (PIC) could not write an interprocess communication (IPC) message to the end of its pipe.

Type Error: An error occurred

Severity error

ASP_PGCP_IPC_PIPE_WRITE_FAILED

System Log Message Unable to write IPC message (type *message-type*, subtype *message-subtype*) to pipe: status code *status*

Description The Packet Gateway Control Protocol (PGCP) client on the MultiServices Physical Interface Card (PIC) could not write the contents of its interprocess communication (IPC) pipe to the socket layer.

Type Error: An error occurred

Severity error

ASP_SFW_ALG_LEVEL_ADJUSTED

System Log Message ALG *sfw-application-name* specified by stateful firewall or CoS rule was reduced to *nat-application-name*, because twice NAT does not support ALG *application*

Description A twice Network Address Translation (NAT) rule is applied to the same source or destination addresses as a stateful firewall or class-of-service (CoS) rule that applies an application-level gateway (ALG) other than Internet Control Message Protocol (ICMP) or traceroute. The configuration is invalid, because only those ALGs are supported in combination with twice NAT. The ALG configured in the stateful firewall or CoS rule was ignored, and only the application configured in the twice-NAT rule was applied. The adaptive services software accomplished this internally by adjusting the indicated ALG value (which is not supported with twice NAT) to the indicated supported value.

Type Event: This message reports an event, not an error

Severity warning

Action Change the configuration so that twice-NAT rules (defined at the [edit services nat] hierarchy level) are not applied to the same source or destination addresses as rules defined at the [edit services stateful-firewall] or [edit services cos] hierarchy level that include ALGs other than the supported ones.

ASP_SFW_ALG_PROMOTION_FAILED

System Log Message ALG promotion failed. Stateful firewall application *sfw-application-name* conflicts with NAT application *nat-application-name* or conflicts with QoS application; request creation of discard flow

Description A matching application-level gateway protocol (ALG) was found from both the indicated stateful firewall rule and either the indicated Network Address Translation (NAT) rule or a quality-of-service (QoS) rule, but the two ALGs were not at the same level.

Type Event: This message reports an event, not an error

Severity critical

Action Resolve the conflicting application-protocol matching conditions in the rules at the [edit services stateful-firewall] hierarchy level and either the [edit services cos] (for QoS rules) or [edit services nat] (for NAT rules) hierarchy level.

ASP_SFW_APP_MSG_TOO_LONG

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because the packet was so large that it exhausted memory resources. The packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

Action Delete active flows to forcibly free memory, or wait for the system to reclaim memory. Consider creating more service sets among which resources can be divided. Otherwise, contact your technical support representative.

ASP_SFW_CHANGE_INACTIVITY_TIMER

System Log Message change global inactivity timer to *value1* open timeout to *value2*

Description The global inactivity timer and the open timeout were set to the indicated values.

Type Event: This message reports an event, not an error

Severity critical

ASP_SFW_CREATE_ACCEPT_FLOW

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type nat-information*

Description The packet with the indicated characteristics matched a stateful firewall rule that has the 'accept' action, and the stateful firewall created a flow. If the flow requires Network Address Translation (NAT) services, NAT information appears at the end of the message. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity info

ASP_SFW_CREATE_DISCARD_FLOW

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The packet with the indicated characteristics matched a stateful firewall rule that has the 'discard' action, and the stateful firewall created a discard flow. The matching packet contained the indicated information about its protocol (numerical identifier

and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_CREATE_REJECT_FLOW

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The packet with the indicated characteristics matched a stateful firewall rule that has the 'reject' action, and the stateful firewall created a reject flow. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_FTP_ACTIVE_ACCEPT

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type nat-information*

Description When the stateful firewall receives PORT/EPRT commands in the control channel, it creates a flow in anticipation of an FTP data connection from client to server. The packet with the indicated characteristics matched such a flow. If the flow requires Network Address Translation (NAT) services, NAT information appears at the end of the message. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_FTP_PASSIVE_ACCEPT

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type nat-information*

Description When the stateful firewall receives PASV/EPSV commands in the control channel, it creates a flow in anticipation of an FTP data connection from server to client. The packet with the indicated characteristics matched such a flow. If the flow requires Network Address Translation (NAT) services, NAT information appears at the end of the message. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_ICMP_ERROR_DROP

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Internet Control Message Protocol (ICMP) error packet with the indicated characteristics, because the packet did not belong to an existing flow. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_ICMP_HEADER_LEN_ERROR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Internet Control Message Protocol (ICMP) packet with the indicated characteristics, because the length field in the packet header was shorter than the minimum 8 bytes required for an ICMP packet. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_ICMP_PACKET_ERROR_LENGTH

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Internet Control Message Protocol (ICMP) error packet with the indicated characteristics, because the packet contained fewer than 48 bytes of data, or more than 576. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_FRAG_ASSEMBLY_TIMEOUT

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and all related IP fragments it had previously received, because all fragments did not arrive within the four-second reassembly timeout period. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_FRAG_OVERLAP

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and all related IP fragments it had previously received, because the contents of two fragments overlapped. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_OPTION_DROP_PACKET

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the packet contained nonconfigured IP option types. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_CHECKSUM_ERROR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the packet checksum was incorrect. The discarded packet contained the indicated

information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_DST_BAD

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the packet destination address was either a multicast address or was in the range reserved for experimental use (248.0.0.0 through 255.255.255.254). The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_FRAG_LEN_INV

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics and all related IP fragments it had previously received, because the length of a fragment was invalid. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_INCORRECT_LEN

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the IP packet with the indicated characteristics, because the packet length was invalid. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_LAND_ATTACK

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the IP packet with the indicated characteristics, because the source and destination address for the packet were the same (referred to as a land attack). The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_NOT_VERSION_4

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the IP packet with the indicated characteristics, because the packet version was not IP version 4 (IPv4). The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_PROTOCOL_ERROR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the IP packet with the indicated characteristics, because the packet used an invalid protocol. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_SRC_BAD

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the packet source address was one of the following: (1) a multicast address (2) a broadcast address (3) in the range 127.0.0.0 through 127.255.255.255 (4) in the range 248.0.0.0 through 255.255.255.254, which is reserved for experimental use.

The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_TOO_LONG

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the IP packet with the indicated characteristics, because the packet contained more than 64 kilobytes (KB) of data (referred to as a ping-of-death attack). The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_TOO_SHORT

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the IP packet with the indicated characteristics, because the packet did not contain the minimum amount of data required. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_IP_PACKET_TTL_ERROR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the IP packet with the indicated characteristics, because the packet had a time-to-live (TTL) value of 0 (zero). The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_NEW_POLICY

System Log Message install new configuration

Description A new stateful firewall policy was installed.

Type Event: This message reports an event, not an error

Severity critical

ASP_SFW_NO_IP_PACKET

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall received the packet with the indicated characteristics, which was not an IP packet. The packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_NO_POLICY

System Log Message *source-address* -> *destination-address*No policy

Description The stateful firewall received packets with the indicated source and destination addresses. There was no matching policy for the traffic.

Type Event: This message reports an event, not an error

Severity critical

ASP_SFW_NO_RULE_DROP

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the packet did not match and stateful firewall rules. In this case, the default action is to discard the packet. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_PING_DUPLICATED_SEQNO

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Internet Control Message Protocol (ICMP) echo request packet with the indicated characteristics, because packet's sequence number was the same as in a previous packet. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_PING_MISMATCHED_SEQNO

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Internet Control Message Protocol (ICMP) echo reply packet with the indicated characteristics, because the firewall had not previously received an echo request packet with the same sequence number. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_PING_OUTOF_SEQNO_CACHE

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Internet Control Message Protocol (ICMP) echo request packet with the indicated characteristics, because it had not received echo replies for an excessive number of previously received echo requests. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_POLICY_REJECT

System Log Message reject configuration because *reason*

Description A newly installed stateful firewall policy was rejected for the indicated reason.

Type Event: This message reports an event, not an error

Severity critical

ASP_SFW_RULE_ACCEPT

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type* rule-set: *rule-set-name*, rule: *rule-name*, term: *term-name*

Description The packet with the indicated characteristics matched the indicated term in the indicated stateful firewall rule, which has an 'accept' action. If the rule belongs to a rule set, the rule set name is also displayed. The stateful firewall accepted the flow to which the packet belongs. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity info

ASP_SFW_RULE_DISCARD

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type* rule-set: *rule-set-name*, rule: *rule-name*, term: *term-name*

Description The packet with the indicated characteristics matched the indicated term in the indicated stateful firewall rule, which has a 'discard' action. If the rule belongs to a rule set, the rule set name is also displayed. The stateful firewall discarded the packet. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_RULE_REJECT

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*) application: *application*, *source-interface-nameseparatorsource-address*:*source-port* -> *destination-addressdestination-port*, *event-type* rule-set: *rule-set-name*, rule: *rule-name*, term: *term-name*

Description The packet with the indicated characteristics matched the indicated term in the indicated stateful firewall rule, which has a 'reject' action. If the rule belongs to a rule set, the rule set name is also displayed. If the packet used the User Datagram Protocol (UDP), the stateful firewall generated an Internet Control Message Protocol (ICMP) error message. If the packet used the Transmission Control Protocol (TCP), the stateful firewall generated an RST packet. The matching packet contained the indicated information about its protocol (numerical identifier and name), application, source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_SYN_DEFENSE

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the Transmission Control Protocol (TCP) handshake that is used to establish a session did not complete quickly enough. The time limit is set by the 'open-timeout' statement at the [edit interfaces < services-interface > services-options] hierarchy level or is four seconds by default. The event was reported to intrusion detection services (IDS) and can cause IDS to activate SYN cookie protection. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

Cause Possible causes for the handshake failure include the following: (1) sequence numbers did not match in a SYN packet and a previous SYN packet (the second packet was not a retransmission) (2) sequence numbers did not match in a SYN/ACK packet and a previous SYN packet (3) either or both a SYN/ACK packet and an ACK packet did not arrive at the firewall within the time limit.

ASP_SFW_TCP_BAD_SYN_COOKIE_RESP

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) ACK packet with the indicated characteristics, either because it is the first packet in a session, or because its sequence number did not match the sequence number in the SYN/ACK packet that the firewall previously generated for the session. The firewall generates SYN/ACK packets when SYN cookie protection is activated. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_TCP_FLAGS_ERROR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because the flags in the packet were set in one of the following combinations: (1) FIN and RST (2) SYN and one or more of FIN, RST, and URG. The discarded packet contained the indicated information about its protocol

(numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_TCP_HEADER_LEN_ERROR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because the length field in the packet header was shorter than the minimum 20 bytes required for a TCP packet. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_TCP_NON_SYN_FIRST_PACKET

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because it was the first packet in the TCP session but the SYN flag was not set. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_TCP_PORT_ZERO

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because the source or destination port specified in the packet was zero (0). The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_TCP_RECONSTRUCT_DROP

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because the session to which the packet belongs violated TCP standards. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

Cause Possible causes include the following: (1) the amount of previously received but unacknowledged data exceeded the TCP window (2) there were sequence number errors (gaps in the sequence or packets with overlapping numbers).

ASP_SFW_TCP_SCAN

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall received a Transmission Control Protocol (TCP) RST packet from a server, indicating that the server rejected a connection attempt directed to the indicated destination address and port. The event was reported to intrusion detection services (IDS) and can cause IDS to activate SYN cookie protection. The RST packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_TCP_SEQNO_AND_FLAGS_ZERO

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because the packet's sequence number was 0 (zero) and no flags were set. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_TCP_SEQNO_ZERO_FLAGS_SET

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the Transmission Control Protocol (TCP) packet with the indicated characteristics, because the packet's sequence number was 0 (zero) and one or more of the FIN, PSH, and RST flags were set. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_UDP_HEADER_LEN_ERROR

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the User Datagram Protocol (UDP) packet with the indicated characteristics, because the length field in the packet header was shorter than the minimum 8 bytes required for an UDP packet. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_UDP_PORT_ZERO

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the User Datagram Protocol (UDP) packet with the indicated characteristics, because the source or destination port specified in the packet was zero (0). The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_UDP_SCAN

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall received an Internet Control Message Protocol (ICMP) error message from a server running at the indicated destination address and User Datagram Protocol (UDP) port. The error packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity notice

ASP_SFW_VERY_BAD_PACKET

System Log Message *syslog-prefix error-code*: proto *protocol-id* (*protocol-name*), *source-interface-nameseparatorsource-address*:*source-port* - > *destination-addressdestination-port*, *event-type*

Description The stateful firewall discarded the packet with the indicated characteristics, because the packet was malformed. The discarded packet contained the indicated information about its protocol (numerical identifier and name), source (logical interface name, IP address, and port number), and destination (IP address and port number).

Type Event: This message reports an event, not an error

Severity critical

ASP_SVC_SET_MAX_FLOWS_EXCEEDED

System Log Message Number of flows (currently *current-flows*) exceeded configured limit (*maximum-value*) *count* times in previous 60 seconds

Description A flow was not created for a service and service set, because the current number of flows for all supported services exceeded the limit configured with the 'max-flows' statement at the [edit services service-set < service-set-name >] hierarchy level. The message appears once per minute and reports the number of times in the previous 60 seconds that the system noted the excessive number of flows.

Type Event: This message reports an event, not an error

Severity notice

Chapter 8

AUDITD System Log Messages

This chapter describes messages with the AUDITD prefix. They are generated by the audit process (auditd), which notifies the RADIUS accounting server of user activity on the routing platform, such as login, logout, and execution of command-line interface (CLI) commands.

AUDITD_RADIUS_AV_ERROR

System Log Message Unable to create *type* record: *error-message*

Description The audit process (auditd) experienced the indicated error when building RADIUS attribute-value (AV) pairs for the indicated type of accounting request, which can be a login or logout event, or a command issued in the CLI.

Type Error: An error occurred

Severity error

AUDITD_RADIUS_OPEN_FAILED

System Log Message *function-name*: unable to create RADIUS object handle (*error-message*)

Description The audit process (auditd) could not create a RADIUS object handle, which it uses for various RADIUS operations.

Type Error: An error occurred

Severity emergency

AUDITD_RADIUS_REQ_CREATE_FAILED

System Log Message Unable to create RADIUS request: *error-message*

Description The audit process (auditd) could not create a RADIUS accounting request for the indicated reason.

Type Error: An error occurred

Severity error

AUDITD_RADIUS_REQ_DROPPED

System Log Message Discarded Accounting-Request message; no RADIUS server responded

Description The audit process (auditd) gathers information about system accounting events from other system processes and sends the information to RADIUS servers in an Accounting-Request message. The process repeatedly sent a message to all configured RADIUS servers without receiving a response, so it discarded the message.

Type Error: An error occurred

Severity error

Cause The RADIUS accounting servers are not correctly configured or are unreachable, or the server applications are not responding.

AUDITD_RADIUS_REQ_SEND_ERROR

System Log Message *function-name*: *error-message*

Description The audit process (auditd) experienced the indicated error when it requested accounting information from a RADIUS server.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

AUDITD_RADIUS_REQ_TIMED_OUT

System Log Message Retransmitted request to RADIUS server *radius-server*

Description The audit process (auditd) gathers information about system accounting events from other system processes and sends the information to RADIUS servers in an Accounting-Request message. After failing to receive a response from the indicated server, auditd waited for a timeout period and resent the message.

Type Error: An error occurred

Severity error

Cause The RADIUS server is not responding. Possible reasons include (a) the server machine is down, too busy, or unreachable (b) the server application is down or too busy (c) the shared RADIUS secret sent by auditd does not match the secret on the server.

AUDITD_RADIUS_SERVER_ADD_ERROR

System Log Message Unable to add RADIUS server *radius-server*: *error-message*

Description The audit process (auditd) read the RADIUS accounting server configuration, but could not add the indicated server to the internal structure used to track servers.

Type Error: An error occurred

Severity error

AUDITD_SOCKET_FAILURE

System Log Message *function-name*: unable to *operation* socket (*error-message*)

Description The audit process (auditd) listens on a Transmission Control Protocol (TCP) socket for system accounting events reported by other processes on the routing platform. The indicated socket operation failed with the indicated error.

Type Error: An error occurred

Severity emergency

Cause An internal software failure occurred.

Action Contact your technical support representative.

Chapter 9

AUTHD System Log Messages

This chapter describes messages with the AUTHD prefix. They are generated by the generic authentication service process (authd).

AUTHD_AUTH_CREATE_FAILED

System Log Message Unable to allocate authentication handle: *error-message*

Description The generic authentication service process (authd) could not allocate an authentication object for the indicated reason.

Type Error: An error occurred

Severity error

AUTHD_RADIUS_GETHOSTNAME_FAILED

System Log Message Unable to obtain hostname for outgoing RADIUS message: *error-message*

Description The generic authentication service process (authd) could not obtain a hostname for an outgoing RADIUS message.

Type Error: An error occurred

Severity error

AUTHD_SERVER_INIT_BIND_FAIL

System Log Message Unable to bind to socket *file-descriptor*: *error-message* (errno *error-code*)

Description The generic authentication service process (authd) could not bind the server to the address specified.

Type Error: An error occurred

Severity error

AUTHD_SERVER_INIT_LISTEN_FAIL

System Log Message Unable to listen on socket *file-descriptor*: *error-message* (errno *error-code*)

Description The generic authentication service process (authd) could not initialize listening on the server for the indicated socket.

Type Error: An error occurred

Severity error

Chapter 10

AUTOD System Log Messages

This chapter describes messages with the AUTOD prefix. They are generated by the autoinstallation process (autod), which controls the initialization of J-series Services Routers.

AUTOD_BIND_FAILURE

System Log Message Unable to bind address to socket: *error-message*

Description The autoinstallation process (autod) received the indicated error when it tried to bind a socket to an address.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

AUTOD_HOSTNAME_EXPANSION_FAILURE

System Log Message Unable to expand compressed DNS domain name: *error-message*

Description The autoinstallation process (autod) received the indicated error when it tried to expand a compressed Domain Name System (DNS) domain name.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

AUTOD_RECV_FAILURE

System Log Message Unable to receive on socket: *error-message*

Description The autoinstallation process (autod) received the indicated error when it tried to receive data on a socket.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

AUTOD_RES_MKQUERY_FAILURE

System Log Message DNS query failed: *error-message*

Description The autoinstallation process (autod) received the indicated error when it made a Domain Name System (DNS) query.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

AUTOD_SEND_FAILURE

System Log Message Unable to send on socket: *error-message*

Description The autoinstallation process (autod) received the indicated error when it tried to send data on a socket.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

AUTOD_SOCKET_CREATE_FAILURE

System Log Message Unable to create socket: *error-message*

Description The autoinstallation process (autod) received the indicated error when it tried to create a socket.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

Chapter 11

AV System Log Messages

This chapter describes messages with the AV prefix. They are generated by the antivirus scanning process (av).

AV_HUGE_FILE_DROPPED

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was dropped because maximum content size was exceeded.

Description The antivirus scanner dropped the received traffic without scanning because the file size exceeded the maximum content limit.

Type Event: This message reports an event, not an error

Severity warning

AV_HUGE_FILE_DROPPED_MT

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was dropped because maximum content size was exceeded.

Description The antivirus scanner dropped the received traffic without scanning because the file size exceeds the maximum content limit; see product Release Notes for the maximum content size supported on a device

Type Event: This message reports an event, not an error

Severity warning

AV_HUGE_FILE_NOT_SCANNED

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was not scanned because maximum content size was exceeded.

Description The antivirus scanner passed the received traffic without scanning because the file size exceeded the maximum content limit.

Type Event: This message reports an event, not an error

Severity warning

AV_HUGE_FILE_NOT_SCANNED_MT

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was not scanned because maximum content size was exceeded.

Description The antivirus scanner passed the received traffic without scanning because the file size exceeds the maximum content limit; see product Release Notes for the maximum content size supported on a device

Type Event: This message reports an event, not an error

Severity warning

AV_MANY_MSGS_DROPPED

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* dropped because the maximum number of concurrent messages was exceeded.

Description The antivirus scanner dropped the received traffic because the maximum number of concurrent messages to scan was exceeded.

Type Event: This message reports an event, not an error

Severity warning

AV_MANY_MSGS_DROPPED_MT

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* dropped because the maximum number of concurrent messages exceeded.

Description The antivirus scanner dropped the received traffic because the maximum number of concurrent messages to scan is exceeded

Type Event: This message reports an event, not an error

Severity warning

AV_MANY_MSGS_NOT_SCANNED

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was not scanned because the maximum number of concurrent messages was exceeded.

Description The antivirus scanner passed the received traffic without scanning because the maximum number of concurrent messages to scan was exceeded.

Type Event: This message reports an event, not an error

Severity warning

AV_MANY_MSGS_NOT_SCANNED_MT

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was not scanned because the maximum number of concurrent messages are exceeded.

Description The antivirus scanner passed the received traffic without scanning because the maximum number of concurrent messages to scan is exceeded

Type Event: This message reports an event, not an error

Severity warning

AV_PATTERN_GET_FAILED

System Log Message AntiVirus: cannot retrieve pattern *error-message* file due to *error-code* (*status-code*).

Description The device was unable to access or retrieve an antivirus pattern file from a server, identified by IP address and port number, through HTTP. The error code provides information you need to get help from Juniper Networks technical support

Type Event: This message reports an event, not an error

Severity notice

Cause Unable to retrieve an antivirus pattern file from the server

Action Contact Juniper Networks technical support

AV_PATTERN_KEY_EXPIRED

System Log Message AntiVirus: Attempt to *time* failed due to *date*, please renew to receive updates.

Description The internal antivirus scanner was unsuccessful in downloading the antivirus pattern file, because the AV license key has been expired

Type Event: This message reports an event, not an error

Severity notice

Cause Download the antivirus pattern file while antivirus license key has been expired

Action Renew the antivirus license key

AV_PATTERN_KL_CHECK_FAILED

System Log Message AntiVirus: db file signature mismatch: *error-message*.

Description The device is unable to use Kaspersky's pattern file. The error message provides information you need to give Juniper Networks technical support

Type Event: This message reports an event, not an error

Severity critical

Cause The device is unable to use Kaspersky's pattern file

Action Contact Juniper Networks technical suppor

AV_PATTERN_TOO_BIG

System Log Message AntiVirus: The pattern file specified in server is too large(*file-size* bytes)

Description The pattern file size specified in the server initialization file (server.ini) exceeds the maximum prescribed limit

Type Event: This message reports an event, not an error

Severity alert

Cause The pattern file size specified in the server initialization file exceeds the limit

Action Contact Juniper Networks technical suppor

AV_PATTERN_UPDATED

System Log Message AntiVirus: Pattern file updated. Version: *version*; size: *file-size* bytes

Description The internal antivirus scanner successfully updated the pattern file and may have changed the size of the file in the process

Type Event: This message reports an event, not an error

Severity notice

Cause The internal antivirus scanner successfully updated the antivirus pattern file

Action No recommended action

AV_PATTERN_WRITE_FS_FAILED

System Log Message AntiVirus: db file save failed: *error-code*

Description The device is unable to save contents of an antivirus pattern file to the file system

Type Event: This message reports an event, not an error

Severity critical

Cause The device is unable to save contents of an antivirus pattern file to the file syste

Action Contact Juniper Networks technical support

AV_SCANNER_DROP_FILE

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was dropped because scan-engine error or constraint with code *error-code* for *error-message*.

Description The antivirus scanner dropped the received traffic because of an internal error.

Type Event: This message reports an event, not an error

Severity warning

AV_SCANNER_DROP_FILE_MT

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was dropped because scan-engine error or constraint with code *error-code* for *error-message*.

Description The antivirus scanner dropped the received traffic because of an internal error

Type Event: This message reports an event, not an error

Severity warning

AV_SCANNER_ERROR_SKIPPED

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was not scanned because scan-engine error or constraint with code *error-code* for *error-message*.

Description The antivirus scanner passed the received traffic because of an internal error.

Type Event: This message reports an event, not an error

Severity warning

AV_SCANNER_ERROR_SKIPPED_MT

System Log Message AntiVirus: Content from *source-address*:*source-port* to *destination-address*:*destination-port filename* was not scanned because scan-engine error or constraint with code *error-code* for *error-message*.

Description The antivirus scanner passed the received traffic because of an internal error

Type Event: This message reports an event, not an error

Severity warning

AV_SCANNER_READY

System Log Message AntiVirus:The scan engine is ready.

Description The antivirus scan engine is ready to scan the traffic

Type Event: This message reports an event, not an error

Severity notice

Cause The antivirus scan engine is ready

Action No recommended action

AV_VIRUS_DETECTED

System Log Message AntiVirus: Virus detected: from *source-address*:*source-port* to *destination-address*:*destination-port filename* file *temporary-filename* virus *name*

Description The antivirus scanner detected a virus. See the log file to see the source and destination port and IP along with contaminated file and virus name.

Type Event: This message reports an event, not an error

Severity warning

AV_VIRUS_DETECTED_MT

System Log Message AntiVirus: Virus detected: from *source-address*:*source-port* to *destination-address*:*destination-port filename* file *temporary-filename* virus *name*

Description The antivirus scanner has detected a virus; the log will show source and destination port and IP along with contaminated file and the virus name

Type Event: This message reports an event, not an error

Severity warning

Chapter 12

BFDD System Log Messages

This chapter describes messages with the BFDD prefix. They are generated by the Bidirectional Forwarding Detection protocol process (bfdd), which detects failures in the bidirectional path between two routing platforms.

BFDD_MIRROR_ERROR

System Log Message Unable to establish BFD mirror connection between Routing Engines: *error-message*

Description The Bidirectional Forwarding Detection process (bfdd) could not establish the mirror connection (which supports nonstop routing) between the master and backup Routing Engines.

Type Error: An error occurred

Severity warning

Cause The master and backup Routing Engines are running incompatible versions of the JUNOS software.

Action Update the JUNOS software to compatible versions on the master and backup Routing Engines.

BFDD_MIRROR_VERSION_MISMATCH

System Log Message Versions of BFD mirror software on Routing Engines are incompatible: *error-message*

Description While trying to establish the mirror connection (which supports nonstop routing) between the master and backup Routing Engines, the Bidirectional Forwarding Detection process (bfdd) determined that the versions of JUNOS software on the Routing Engines were incompatible.

Type Error: An error occurred

Severity warning

Action Update the JUNOS software to compatible versions on the master and backup Routing Engines.

BFDD_READ_ERROR

System Log Message Read error on *pipe-type* pipe: *reason* (*error-message*)

Description The Bidirectional Forwarding Detection process (bfdd) could not read the message available on the indicated type of pipe.

Type Error: An error occurred

Severity info

Action Contact your technical support representative.

BFDD_TRAP_STATE_DOWN

System Log Message local discriminator: *session-id*, new state: *state*

Description The state changed to 'down' or 'admin down' for the indicated Bidirectional Forwarding Detection process (bfdd) session.

Type Event: This message reports an event, not an error

Severity warning

BFDD_TRAP_STATE_UP

System Log Message local discriminator: *session-id*, new state: *state*

Description The state changed to 'up' for the indicated Bidirectional Forwarding Detection process (bfdd) session.

Type Event: This message reports an event, not an error

Severity info

BFDD_WRITE_ERROR

System Log Message *function-name*: write error on *pipe-type* pipe (*error-message*)

Description The Bidirectional Forwarding Detection process (bfdd) could not write a message to the indicated type of pipe.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

Chapter 13

BOOTPD System Log Messages

This chapter describes messages with the BOOTPD prefix. They are generated by the boot parameter process (tnp.bootpd), which provides the appropriate boot string to hardware components as they initialize.

BOOTPD_ARG_ERR

System Log Message Ignoring unknown option *-option*

Description The indicated option was provided on the 'tnp.bootpd' command line and is invalid. The boot parameter process (tnp.bootpd) initialized but ignored the invalid option.

Type Error: An error occurred

Severity warning

Action Remove the invalid option from the 'tnp.bootpd' command line.

BOOTPD_BAD_ID

System Log Message Unexpected ID 0x*assembly-id*

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). The boot strings are defined in the configuration file tnp.bootpd. A request failed because it included the indicated assembly ID, for which there is no definition in the file.

Type Event: This message reports an event, not an error

Severity notice

BOOTPD_BOOTSTRING

System Log Message Boot string: *boot-string*

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). tnp.bootpd responded with the indicated boot string.

Type Event: This message reports an event, not an error

Severity info

BOOTPD_CONFIG_ERR

System Log Message Problems with configuration file '*filename*', using defaults

Description The boot parameter process (tnp.bootpd) could not read the indicated configuration file, so it initialized using default settings defined at compile time.

Type Error: An error occurred

Severity error

Action Correct the configuration file.

BOOTPD_CONF_OPEN

System Log Message Unable to open configuration file '*filename*'

Description The boot parameter process (tnp.bootpd) could not open the indicated configuration file, so it initialized using default settings defined at compile time.

Type Event: This message reports an event, not an error

Severity notice

Action Contact your technical support representative.

BOOTPD_DUP_PIC_SLOT

System Log Message Duplicate default value defined for PIC *pic-slot* in FPC *fpc-slot*

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). The boot strings are defined in the configuration file for tnp.bootpd. There was more than one definition in the file for the indicated Physical Interface Card (PIC) slot in the indicated Flexible PIC Concentrator (FPC), so tnp.bootpd used the first definition it found.

Type Event: This message reports an event, not an error

Severity notice

Action Remove the extra definitions from the configuration file.

BOOTPD_DUP_REV

System Log Message Duplicate revision: *major-version.minor-version*

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). The boot strings are defined in the configuration file for tnp.bootpd. There was more than one definition in the file for the indicated revision of a component, so tnp.bootpd used the first definition it found.

Type Event: This message reports an event, not an error

Severity notice

Action Remove the extra definitions from the configuration file.

BOOTPD_DUP_SLOT

System Log Message Duplicate slot default: *slot*

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). The boot strings are defined in the configuration file for tnp.bootpd. There was more than one definition in the file for the indicated slot (combination of component assembly ID and revision), so tnp.bootpd used the first definition it found.

Type Event: This message reports an event, not an error

Severity notice

Action Remove the extra definitions from the configuration file.

BOOTPD_HWDB_ERROR

System Log Message Operation in chassis hardware database failed: *error-message*

Description The boot parameter process (tnp.bootpd) could not complete an operation in the hardware database maintained by the chassis process (chassisd), for the indicated reason.

Type Error: An error occurred

Severity error

BOOTPD_MODEL_CHK

System Log Message Unexpected ID 0x*identifier* for model *model*

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). A request failed because it included the indicated assembly ID, which is inconsistent with the routing platform's model number.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

BOOTPD_MODEL_ERR

System Log Message Unsupported model *model*, assuming M40 defaults

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). The boot strings are defined in the configuration file for tnp.bootpd. A request included a model number for which there was no definition in the configuration file, so tnp.bootpd provided the boot string appropriate for an M40 router.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

BOOTPD_NEW_CONF

System Log Message New configuration installed

Description The boot parameter process (tnp.bootpd) loaded a new configuration file.

Type Event: This message reports an event, not an error

Severity info

BOOTPD_NO_BOOTSTRING

System Log Message No boot string found for type *board-type major-version.minor-version command-type*

Description As each hardware component on the routing platform initializes, it requests a boot string from the boot parameter process (tnp.bootpd). The boot strings are defined in the configuration file for tnp.bootpd. The file did not include a boot string for the hardware component with the indicated characteristics.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

BOOTPD_NO_CONFIG

System Log Message No configuration file '*filename*', using defaults

Description The boot parameter process (tnp.bootpd) could not open the indicated configuration file, so it initialized using default settings defined at compile time.

Type Event: This message reports an event, not an error

Severity notice

BOOTPD_PARSE_ERR

System Log Message *filename*: *return-value* parse errors on SIGHUP

Description There was an error in the configuration file for the boot parameter process (tnp.bootpd), so it initialized using default settings defined at compile time.

Type Error: An error occurred

Severity error

Action Correct the configuration file.

BOOTPD_REPARSE

System Log Message Reparsing configuration file '*filename*'

Description The boot parameter process (tnp.bootpd) reparsed the indicated configuration file.

Type Event: This message reports an event, not an error

Severity info

BOOTPD_SELECT_ERR

System Log Message select: *error-message*

Description The boot parameter process (tnp.bootpd) issued the select() system call, which returned the indicated error message.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

BOOTPD_TIMEOUT

System Log Message Timeout *duration* unreasonable

Description The indicated timeout value was specified for the -t argument on the 'tnp.bootpd' command line, or no value was provided. The value was not acceptable, so the boot parameter process (tnp.bootpd) initialized using the default value of 30 seconds.

Type Error: An error occurred

Severity warning

Action Provide an acceptable value for the -t argument; acceptable values are '1' (second) and larger.

Chapter 14

CFMD System Log Messages

This chapter describes messages with the CFMD prefix. They are generated by the connectivity-fault management (CFM) process (cfmd), which supports Operation, Administration, and Maintenance (OAM) functions that are defined in the Institute of Electrical and Electronics Engineers (IEEE) 802.1ag standard for Ethernet interfaces.

CFMD_CCM_DEFECT_CROSS_CONNECT

System Log Message CFM defect: *error-message*

Description A connectivity-fault management (CFM) maintenance endpoint (MEP) received a continuity check message (CCM) that had an incorrect maintenance association (MA) ID or a maintenance domain (MD) level lower than that of the MEP, each of which indicates a cross-connect error.

Type Event: This message reports an event, not an error

Severity error

Cause The configuration is invalid.

Action Check whether the configured MD name, format, and level, or the MA name or format, is different from the remote endpoint.

CFMD_CCM_DEFECT_ERROR

System Log Message CFM defect: *error-message*

Description A connectivity-fault management (CFM) maintenance endpoint (MEP) received a continuity check message (CCM) with an incorrect transmission interval or MEP ID, which indicates a configuration error.

Type Event: This message reports an event, not an error

Severity error

Cause The configuration is invalid.

Action Verify that the configured continuity-check transmission interval does not differ from the remote endpoint, and that the configured MEP ID is valid.

CFMD_CCM_DEFECT_MAC_STATUS

System Log Message CFM defect: *error-message*

Description A connectivity-fault management (CFM) maintenance endpoint (MEP) received a continuity check message (CCM) that contained a 'Port Status' or 'Interface Status' type, length, value (TLV), which indicate a failed bridge port or aggregated port.

Type Event: This message reports an event, not an error

Severity error

CFMD_CCM_DEFECT_NONE

System Log Message CFM defect: *error-message*

Description No defect was detected.

Type Event: This message reports an event, not an error

Severity error

CFMD_CCM_DEFECT_RDI

System Log Message CFM defect: *error-message*

Description A connectivity-fault management (CFM) maintenance endpoint (MEP) received a continuity check message (CCM) that had the 'Remote Defect Indication' (RDI) bit set, which indicates that not all configured MEPs are returning CCMs to the transmitting MEP.

Type Event: This message reports an event, not an error

Severity error

CFMD_CCM_DEFECT_RMEP

System Log Message CFM defect: *error-message*

Description A connectivity-fault management (CFM) maintenance endpoint (MEP) did not receive three consecutive continuity check message (CCM)s from one of the other MEPs in its maintenance association (MA), which indicates a MEP failure or network failure.

Type Event: This message reports an event, not an error

Severity error

CFMD_CCM_DEFECT_UNKNOWN

System Log Message CFM defect: *error-message*

Description An unknown defect was detected.

Type Event: This message reports an event, not an error

Severity error

Chapter 15

CHASSISD System Log Messages

This chapter describes messages with the CHASSISD prefix. They are generated by the chassis process (chassisd), which controls hardware components on the routing platform.

CHASSISD_ANTICF_PIM_CHECK_FAILED

System Log Message PIM *pim-slot* failed anti-counterfeit check

Description The indicated Physical Interface Module (PIM) failed the anti-counterfeit check performed by the chassis process (chassisd).

Type Error: An error occurred

Severity error

CHASSISD_ANTICF_RE_CHECK_FAILED

System Log Message Routing Engine failed anti-counterfeit check

Description The Routing Engine failed the anti-counterfeit check performed by the chassis process (chassisd).

Type Error: An error occurred

Severity error

CHASSISD_ANTICF_RE_ROM_READ_FAIL

System Log Message Unable to read serial number from anti-counterfeit device for Routing Engine

Description The chassis process (chassisd) could not read the serial number recorded in the ROM of the anti-counterfeit device for the Routing Engine.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_ANTICF_RE_SHA_READ_FAIL

System Log Message Unable to read SHA output from anti-counterfeit device for Routing Engine

Description The chassis process (chassisd) could not read Secure Hash Algorithm (SHA) information from the anti-counterfeit device for the Routing Engine.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_ANTICF_ROM_READ_FAILED

System Log Message Unable to read serial number from anti-counterfeit device for PIM *pim-slot*

Description The chassis process (chassisd) could not read the serial number recorded in the ROM of the anti-counterfeit device for the indicated Physical Interface Module.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_ANTICF_SHA_READ_FAILED

System Log Message Unable to read SHA output from anti-counterfeit device for PIM *pim-slot*

Description The chassis process (chassisd) could not read Secure Hash Algorithm (SHA) information from the anti-counterfeit device for the indicated Physical Interface Module (PIM).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_ARGUMENT_ERROR

System Log Message Unknown option *option*

Description The indicated option, provided on the 'chassisd' command line, is invalid. The chassis process (chassisd) initialized but ignored the invalid option.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_BLOWERS_SPEED

System Log Message Fans and impellers are now running at normal speed

Description The fans (and impellers, if applicable) were running at the normal speed.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_BLOWERS_SPEED_FULL

System Log Message Fans and impellers being set to full speed [*reason*]

Description For the indicated reason, the chassis process (chassisd) increased the speed of fans (and impellers, if applicable) to the maximum.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_BLOWERS_SPEED_MEDIUM

System Log Message Fans and impellers being set to intermediate speed

Description The chassis process (chassisd) increased the speed of fans (and impellers, if applicable) to the intermediate level because of a temperature increase in the chassis.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_BUS_DEVICE_OPEN_FAILURE

System Log Message Unable to open '*bus-type*' bus device, error *error-message* (*error-code*)

Description The chassis process (chassisd) could not open the indicated bus device for the indicated reason.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_CB_CLOCK_CHECKSUM

System Log Message Clock module on M120 CB had configuration data checksum error

Description The chassis process (chassisd) detected a checksum error for the clock module on an M120 Control Board (CB).

Type Error: An error occurred

Severity error

CHASSISD_CB_MASTER_BP_IGNORED

System Log Message Press of online/offline button ignored for master *fru-name fru-slot*

Description The online/offline button for the indicated control board was pressed, but the chassis process (chassisd) ignored the request. The control board for M40e and M160 routers is the Miscellaneous Control Subsystem (MCS). The control board for M320, T320, and T640 routing platforms is the Control Board (CB).

Type Event: This message reports an event, not an error

Severity error

Cause The control board was acting as master.

Action Switch mastership to the other control board before taking the control board offline.

CHASSISD_CB_READ

System Log Message Error reading midplane ID EEPROM, errno *error-code*

Description The chassis process (chassisd) could not read the EEPROM on the midplane.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_CB_RE_ONLINE_BP_IGNORED

System Log Message Unable to take *fru-name fru-slot* offline because paired Routing Engine is online

Description The online/offline button for the indicated control board was pressed, but the chassis process (chassisd) ignored the request. The control board for M40e and M160 routers is the Miscellaneous Control Subsystem (MCS). The control board for M320, T320, and T640 routing platforms is the Control Board (CB).

Type Event: This message reports an event, not an error

Severity error

Cause The Routing Engine paired with the indicated control board is still online.

Action Take the Routing Engine offline before taking the control board offline.

CHASSISD_CFEB_POWER_FAILURE

System Log Message *function-name*: unable to turn *state* power for CFEB *cfeb-slot*

Description The chassis process (chassisd) could not turn on or turn off the power to the indicated Compact Forwarding Engine Board (CFEB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_CLEAR_CONFIG_ERROR

System Log Message *function-name*: *status*

Description The chassis process (chassisd) encountered an error while trying to clear the state information associated with a copy of the management process (mgd) that it spawned

to commit the rescue configuration. The commit operation succeeded or failed as indicated.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

CHASSISD_CLOCK_FAILURE

System Log Message *function-name*: *fru-name error-message*

Description The chassis process (chassisd) determined that the indicated clock source failed in the indicated way.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_CLOCK_NOTICE

System Log Message *fru-name*: *message*

Description The clock-synchronization status of the indicated component (field-replaceable unit, or FRU) changed as indicated.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_CMB_READBACK_ERROR

System Log Message Readback error from chassis management bus for *fru-name fru-slot* ([0x*address*, 0x*offset*] -> 0x*error-code*)

Description The chassis process (chassisd) could not read back information from the Chassis Management Bus (CMB) about the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Cause The probable cause is hardware error.

Action Contact your technical support representative.

CHASSISD_COMMAND_ACK_ERROR

System Log Message Error occurred when *fru-name fru-slot* reported its online status: *error-message* (error code *error-code*)

Description The chassis process requested that the indicated component (field-replaceable unit, or FRU) confirm that it was online. The indicated error occurred when the FRU sent its response. In the normal case, the chassis process performed any additional action necessary to guarantee that the FRU came online.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_COMMAND_ACK_SFM_ERROR

System Log Message *function-name*: SFM *sfm-slot* did not acknowledge FPC *fpc-slot*: error *error-message* (code *error-code*)

Description The chassis process (chassisd) requires an acknowledgment from each Switching and Forwarding Module (SFM) before it registers a Flexible PIC Controller (FPC) as online. The acknowledgment message from the indicated SFM failed for the indicated FPC.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_CONCAT_MODE_ERROR

System Log Message Cannot set no-concatenated mode for FPC *fpc-slot* PIC *pic-slot*

Description The chassis process (chassisd) could not set channelized mode for the indicated SONET/SDH Physical Interface Card (PIC). Channelized mode is configured by including the no-concatenate statement at the [edit chassis fpc 'slot' pic 'slot'] hierarchy level.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_CONFIG_ACCESS_ERROR

System Log Message *function-name*: *error-message*

Description The chassis process (chassisd) experienced the indicated problem while attempting to parse the configuration database.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

CHASSISD_CONFIG_INIT_ERROR

System Log Message Unable to parse configuration; using defaults

Description The chassis process (chassisd) could not parse the configuration, and used default values while initializing.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_CONFIG_WARNING

System Log Message *function-name*: *warning-message*, FPC *fpc-slot* PIC *pic-slot*

Description The configuration that was specified for the indicated Physical Interface Card (PIC) is invalid for that type of PIC.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_DEVICE_OPEN_ERROR

System Log Message Unable to open *device-name* device file (errno *error-code*)

Description The chassis process (chassisd) could not open the device file for the indicated device.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_EXEC_ERROR

System Log Message *function-name*: *error-message*

Description While trying to commit the rescue configuration, the chassis process (chassisd) encountered an error.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

CHASSISD_EXISTS

System Log Message chassisd already running; exiting

Description The chassis process (chassisd) exited because it discovered that another chassisd process was already running.

Type Event: This message reports an event, not an error

Severity error

CHASSISD_EXISTS_TERM_OTHER

System Log Message Killing existing chassisd and exiting

Description The chassis process (chassisd) discovered that another chassisd process was already running. It terminated the other process and exited.

Type Event: This message reports an event, not an error

Severity error

CHASSISD_FAN_FAILURE

System Log Message *fru-name* in slot *fru-slot* failed

Description The indicated fan or impeller failed. The chassis process (chassisd) raised an alarm and increased the speed of the remaining fans (and impellers, if applicable) to full speed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_CONFIG_COMPLETE

System Log Message Fchip: configuration already completed

Description The chassis process (chassisd) detected an attempt to configure an F chip on a Control Board (CB) when configuration was already complete.

Type Error: An error occurred

Severity error

CHASSISD_FASIC_FTOKEN_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): ftoken overflow/underflow set (*data*) at *address*

Description The chassis process (chassisd) detected an underflow or overflow error on the indicated F chip on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_FTOKEN_INIT_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): f8chip_ftoken_init() stuck in ftoken loop, addr = *address*, data = *data*

Description The chassis process (chassisd) encountered an error while initializing memory at the indicated address for the indicated F chip on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_HSL_CONFIG_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): HSL configuration failed (error *error-message*)

Description The chassis process (chassisd) could not configure high speed links (HSL) for the indicated F chip on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

CHASSISD_FASIC_HSL_LINK_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): link *link-id* failed because of *error-message*

Description The chassis process (chassisd) detected an error for the indicated high speed link (HSL) for the indicated F chip on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_INIT_ERROR

System Log Message Fchips were not configured yet

Description The chassis process (chassisd) detected that F chips were not yet initialized on the Control Board (CB).

Type Error: An error occurred

Severity error

CHASSISD_FASIC_INPUT_DROP

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): dropped *drop-rate* cells per second coming from Packet Forwarding Engine *pfe* on FPC *fpc-slot*

Description The Packet Forwarding Engine divides packets into smaller units called cells for more efficient processing. As the indicated F chip on the indicated Control Board (CB) processed data that was received from the indicated Packet Forwarding Engine on

the indicated Flexible PIC Concentrator (FPC), it dropped the indicated number of cells per second.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_OUTPUT_DROP

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): dropped *drop-rate* cells per second destined for Packet Forwarding Engine *pfe* on FPC *fpc-slot*

Description The Packet Forwarding Engine divides packets into smaller units called cells for more efficient processing. As the indicated F chip on the indicated Control Board (CB) processed data before sending it to the indicated Packet Forwarding Engine on the indicated Flexible Port Concentrator (FPC) for outgoing transmission, it dropped the indicated number of cells per second.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_PIO_READ_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): read error in *function-name*() for link#*link-id* at address *address* in register *register*

Description The indicated routine failed with a read error at the indicated address and register for the indicated F chip and link on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

CHASSISD_FASIC_PIO_WRITE_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): write error in *function-name*() for link#*link-id* at address *address* in register *register*

Description The indicated routine failed with a write error at the indicated address and register for the indicated F chip and link on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

CHASSISD_FASIC_PLL_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): unable to lock PLL

Description The chassis process (chassisd) could not lock a phased-lock loop (PLL) for the indicated F chip on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_RESET_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): reset failed

Description The chassis process (chassisd) could not reset the indicated F chip on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FASIC_SRAM_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): SRAM fuse did not initialize

Description The chassis process (chassisd) detected that static RAM (SRAM) did not initialize properly for the indicated F chip on the indicated Control Board (CB).

Type Error: An error occurred

Severity error

CHASSISD_FASIC_VERSION_ERROR

System Log Message Fchip (CB *control-board-slot*, ID *fchip-id*): part number *part-number* and version *version* were invalid

Description The indicated part number and version detected for the indicated F chip on the indicated Control Board (CB) were not valid values.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_CONFIG_COMPLETE

System Log Message Fchip: configuration already completed

Description The chassis process (chassisd) detected an attempt to configure an F chip when configuration was already complete.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_CONFIG_MD_ERROR

System Log Message Fchip *fchip-id*: invalid number of Md chips (*count*) for Packet Forwarding Engine *pfe* on FPC *fpc-slot*

Description The chassis process (chassisd) detected an invalid number of Md chips for the indicated F chip, Packet Forwarding Engine and Flexible PIC Concentrator (FPC).

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_CONFIG_RATE_ERROR

System Log Message Fchip *fchip-id*: unable to set rate limit on port *port*

Description The chassis process (chassisd) could not set the rate limit for the indicated F chip and port.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_CONFIG_READ_ERROR

System Log Message Fchip *fchip-id*: unable to read configuration register

Description The chassis process (chassisd) could not read a configuration register on the indicated F chip.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_FTOKEN_ERROR

System Log Message Fchip *fchip-id*: Ftoken overflow/underflow set (*data*) at *address*

Description The chassis process (chassisd) detected an underflow or overflow error on the indicated F chip.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FCHIP_FTOKEN_INIT_ERROR

System Log Message Fchip *fchip-id*: fchip_ftoken_init() stuck in ftoken loop, addr = *address*, data = *data*

Description The chassis process (chassisd) encountered an error while initializing memory at the indicated address for the indicated F chip.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FCHIP_HSR_ERROR

System Log Message Fchip high-speed receiver (HSR) error: *error-message*

Description The chassis process (chassisd) detected an error in the high-speed receiver (HSR) subsystem for the F chip with the indicated characteristics.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_HSR_INIT_ERROR

System Log Message HSR: No vectors supplied

Description The chassis process (chassisd) could not initialize the high-speed receiver (HSR) subsystem for an F chip.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_HSR_INIT_LINK_ERR

System Log Message Fchip *fchip-id*: unable to initialize HSR link *link-id*

Description The chassis process (chassisd) could not initialize the indicated high-speed receiver (HSR) link for the indicated F chip.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_HSR_RESET_ERROR

System Log Message Fchip *fchip-id*: hsr_reset error in fchip_init() on link *link-id*

Description A high-speed receiver (HSR) reset error occurred during initialization of the indicated F chip and link.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_HST_ERROR

System Log Message Fchip high-speed transmitter (HST) error: *error-message*

Description The chassis process (chassisd) detected an error in the high-speed transmitter (HST) subsystem for the F chip with the indicated characteristics.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_HST_INIT_ERROR

System Log Message HST: No vectors supplied

Description The chassis process (chassisd) could not initialize the high-speed transmitter (HST) subsystem for an F chip.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_HST_INIT_LINK_ERR

System Log Message Fchip *fchip-id*: unable to initialize HST link *link-id*

Description The chassis process (chassisd) could not initialize the indicated high-speed transmitter (HST) link for the indicated F chip.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_HST_RESET_ERROR

System Log Message Fchip *fchip-id*: hst_reset error in fchip_init() on link *link-id*

Description A high-speed transmitter (HST) reset error occurred during initialization of the indicated F chip and link.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_INIT_ERROR

System Log Message Fchips were not configured yet

Description The chassis process (chassisd) detected that F chips were not yet initialized.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_LINK_ERROR

System Log Message SIB*sib-slot*_F0: *link-type* link *link-id* was bad

Description The chassis process (chassisd) detected an error for the indicated high-speed receiver (HSR) or high-speed transmitter (HST) link for an F chip on the indicated Switch Interface Board (SIB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FCHIP_MONITOR_ERROR

System Log Message F chip module was invalid

Description The chassis process (chassisd) detected an invalid F-chip module while enabling or disabling the monitoring of F-chip functional blocks.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FCHIP_PIO_READ_ERROR

System Log Message Fchip *fchip-id*: read error in *function-name*() for link#*link-id*, at address *address* in register *register*

Description The indicated routine failed with a read error at the indicated address and register for the indicated F chip and link.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_PIO_WRITE_ERROR

System Log Message Fchip *fchip-id*: write error in *function-name*() for link#*link-id*, at address *address* in register *register*

Description The indicated routine failed with a write error at the indicated address and register for the indicated F chip and link.

Type Error: An error occurred

Severity error

CHASSISD_FCHIP_POLL_ERROR

System Log Message Fchip *fchip-id*: *link-type link-id* poll returned error *error-code*

Description An error with the indicated error number occurred during polling of the indicated high-speed receiver (HSR) or high-speed transmitter (HST) link for the indicated F chip.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FCHIP_RATE_ERROR

System Log Message Fchip *fchip-id*: per-port rate limit was not enabled

Description The chassis process (chassisd) detected that per-port rate limiting was not enabled when it attempted to set the rate limit on an individual port for the indicated F chip.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FCHIP_SIB_NOT_STARTED

System Log Message Unable to start *fru-name fru-slot* because F chips were not initialized

Description The indicated Switch Interface Board (SIB) did not start because the F chips on it were not initialized.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FCHIP_VERSION_ERROR

System Log Message F chip *fchip-id*: part number (*part-number*) and version (*version*) were invalid

Description The indicated part number and version detected for the indicated F chip were not valid values.

Type Error: An error occurred

Severity error

CHASSISD_FHSR_READ_REG_ERROR

System Log Message Fchip: fhsr_read() failed at address *address*

Description The high-speed receiver (HSR) read routine failed at the indicated address on an F-chip register.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FHSR_WRITE_REG_ERROR

System Log Message Fchip: fhsr_write() of value *value* failed at address *address*

Description The high-speed receiver (HSR) write routine could not record the indicated value at the indicated address on an F-chip register.

Type Error: An error occurred

Severity error

CHASSISD_FHST_READ_REG_ERROR

System Log Message Fchip: fhst_read() failed at address *address*

Description The high-speed transmitter (HST) read routine failed at the indicated address on an F-chip register.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FHST_WRITE_REG_ERROR

System Log Message Fchip: fhst_write() of value *value* failed at address *address*

Description The high-speed transmitter (HST) write routine could not record the indicated value at the indicated address on an F-chip register.

Type Error: An error occurred

Severity error

CHASSISD_FILE_OPEN

System Log Message File open: *filename*, error: *error-code -- error-message*

Description The chassis process (chassisd) could not open the indicated file for the indicated reason.

Type Error: An error occurred

Severity critical

CHASSISD_FILE_STAT

System Log Message File stat: *filename*, error: *error-code -- error-message*

Description The chassis process (chassisd) could not open the indicated file because it could not obtain its status.

Type Error: An error occurred

Severity error

CHASSISD_FM_BAD_STATE

System Log Message *function-name*: unexpected state *statetype* for SIB#*sib-slot*

Description The indicated function failed because it encountered the indicated type of unexpected internal state with respect to the indicated Switch Interface Board (SIB).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_ERROR

System Log Message *function-name*: *error-message* (SIB#*sib-slot*, Packet Forwarding Engine *pfe* on FPC *fpc-slot*)

Description During execution of the indicated fabric management routine, the indicated error occurred between the indicated Switch Interface Board (SIB) and the indicated Packet Forwarding Engine on the indicated Flexible PIC Concentrator (FPC).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_ERROR_SIB_L_FB_HSR

System Log Message FM: HSR error occurred on link from SIB-S port F(*s-row*,*s-port*) to SIB-L#*sib-slot* port F(*l-row*,*l-port*)

Description In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the T640 routing nodes (called SIB-Ls) and the SIBs in the TX Matrix platform (called SIB-Ss). The chassis process (chassisd) on the routing node that houses the indicated SIB-L detected an error in the electrical path between the indicated ports on the SIB-L and the corresponding SIB-S.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_ERROR_SIB_L_FB_SMF

System Log Message FM: *error-message* error occurred on link *to-from-sib* SIB-L#*sib-slot to-from-scc* SCC

Description In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the TX Matrix platform (the switch-card chassis, or SCC) and the SIBs in the T640 routing nodes (called SIB-Ls). The chassis process (chassisd) on the routing node that houses the indicated SIB-L detected the indicated error as packets that were traveling in the indicated direction were translated between electrical and optical media.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_ERROR_SIB_L_MISMATCH

System Log Message FM: fiber cable from SIB-L#*sib-slot* possibly connected to wrong SIB-S

Description In a routing matrix, the fiber-optic cable between each Switch Interface Board in a T640 routing node (called a SIB-L) must connect to a specific SIB port on the TX Matrix platform (called a SIB-S). The cable originating at the indicated SIB-L was possibly plugged into the wrong SIB-S port or wrong SIB-S.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_ERROR_SIB_S_FB_HSR

System Log Message FM: HSR error occurred on link from LCC*lcc* SIB-L port F(*l-row*,*l-port*) to SIB-S#*sib-slot* port F(*s-row*,*s-port*)

Description In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the TX Matrix platform (called SIB-Ss) and the SIBs in the T640 routing nodes (called SIB-Ls). The chassis process (chassisd) on the TX Matrix platform detected an error in the electrical path between the indicated port on the indicated SIB-S and the indicated port on a SIB-L installed in the indicated routing node (line-card chassis, or LCC).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_ERROR_SIB_S_FB_SMF

System Log Message FM: *error-message* error occurred on link *to-from-sib-s* SIB-S#*sib-slot to-from-lcc* LCC*lcc*

Description In a routing matrix, packets traverse both electrical and optical media as they travel between the Switch Interface Boards (SIBs) in the TX Matrix platform (called SIB-Ss) and the SIBs in the T640 routing nodes (line-card chassis, or LCCs). The chassis process (chassisd) on the TX Matrix platform detected the indicated error as packets that were traveling to or from the indicated LCC were translated between electrical and optical media.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_MEMORY_ERROR

System Log Message *function-name*: unable to allocate memory; *error-message*

Description The chassis process (chassisd) could not allocate memory for a fabric operation.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

CHASSISD_FM_SIB_ERROR

System Log Message Fabric management error for SIB *sib-slot*: *error-message*

Description The chassis process (chassisd) detected the indicated type of error on the indicated Switch Interface Board (SIB) and performed the indicated action.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_SIB_FPC_TYPE_ERROR

System Log Message SIB *sib-slot* does not support features required for FPC Type 4

Description The indicated Switch Interface Board (SIB) does not support features required by the Flexible PIC Concentrator (FPC) Type 4.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FM_SIB_TYPE_ERROR

System Log Message *function-name*: SIB *sib-slot* does not support configured features. But six_slot *state* configured. Correct the configuration and restart chassisd.

Description The configuration that was specified for the indicated Switch Interface Board (SIB) is not supported.

Type Error: An error occurred

Severity error

Action Change the configuration and restart the chassis process (chassisd).

CHASSISD_FPC_NOT_FOUND

System Log Message *function-name*: unable to find FPC for PIC attachment operation

Description The chassis process (chassisd) attempted to bring a Physical Interface Card (PIC) online, but could not find the Flexible PIC Concentrator (FPC) that houses it.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

CHASSISD_FPC_PIC_DETECT_TIMEOUT

System Log Message *function-name*: PIC detection on FPC *fpc-slot* timed out

Description The chassis process (chassisd) expects to receive notification within a timeout period that each Flexible PIC Concentrator (FPC) has attached the Physical Interface Cards (PICs) that it houses. It did not receive notification from the indicated FPC.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FPC_TYPE_SIB_TYPE_ERROR

System Log Message Installed SIB type (SIB-I8-F16) does not support features required by FPC *fpc-slot*

Description The indicated Flexible PIC Concentrator (FPC) is Type 4, which is not supported by Switch Interface Board (SIB) type SIB-I8-F16.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FRU_ALREADY_OFFLINE

System Log Message *fru-name fru-slot* already offline

Description The chassis process (chassisd) received a request to take the indicated component (field-replaceable unit, or FRU) offline, but the FRU was already offline.

Type Event: This message reports an event, not an error

Severity error

CHASSISD_FRU_ALREADY_ONLINE

System Log Message Received request to bring *fru-name fru-slot* online; it was already online

Description The chassis process (chassisd) received a request to bring the indicated component (field-replaceable unit, or FRU) online, but the FRU was already online.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_FRU_EVENT

System Log Message *function-name*: *state fru-name fru-slot*

Description The state of the indicated component (field-replaceable unit, or FRU) changed as indicated.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_FRU_INVALID_SLOT

System Log Message FRU *fru-name* is not supported in current slot

Description The chassis process (chassisd) detected that the indicated hardware component (field-replaceable unit, or FRU) was inserted in a slot that is not valid for that component type.

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

CHASSISD_FRU_IO_ERROR

System Log Message *function-name*: *fru-name operation* error: *reason* (*error-message*)

Description The chassis process (chassisd) could not perform the indicated I/O operation on the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FRU_IO_OFFSET_ERROR

System Log Message *function-name*: *fru-name operation* error: *reason* 0x*offset* (*error-message*)

Description The chassis process (chassisd) could not perform the indicated I/O operation at the indicated byte offset.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_FRU_IPC_WRITE_ERROR

System Log Message *function-name*: FRU *fru-name*, errno *error-code*, *error-message*

Description The chassis process (chassisd) could not send an interprocess communication (IPC) message to the indicated component (field-replaceable unit, or FRU) because of the indicated error.

Type Error: An error occurred

Severity warning

CHASSISD_FRU_OFFLINE_FAILED

System Log Message Unable to take *fru-name fru-slot* offline because FRU sequencer is active: *reason*

Description The chassis process (chassisd) could not take the indicated component (field-replaceable unit, or FRU) offline for the indicated reason.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_FRU_OFFLINE_NOTICE

System Log Message Taking *fru-name fru-slot* offline: *reason*

Description The chassis process (chassisd) took the indicated component (field-replaceable unit, or FRU) offline for the indicated reason.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_FRU_OFFLINE_TIMEOUT

System Log Message Offline request timed out; *fru-name fru-slot* restarted

Description The indicated component (field-replaceable unit, or FRU) did not go offline within the time period that is normally sufficient for synchronized shutdown. After generating this message, the chassis process (chassisd) tried several times to take the FRU offline and powered it down if all attempts failed.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_FRU_ONLINE_TIMEOUT

System Log Message *function-name*: attempt to bring *fru-name fru-slot* online timed out

Description The indicated component (field-replaceable unit, or FRU) did not come online within the time that is normally sufficient. After generating this message, the chassis process (chassisd) tried to bring the FRU online several more times. If all attempts failed, the chassisd process raised an alarm and left the FRU offline.

Type Event: This message reports an event, not an error

Severity error

CHASSISD_FRU_STEP_ERROR

System Log Message *fru-name fru-slot* at step *step-number*

Description The power-on sequence for the indicated component (field-replaceable unit, or FRU) failed at the indicated point.

Type Error: An error occurred

Severity error

CHASSISD_FRU_UNRESPONSIVE

System Log Message Error for *fru-name fru-slot*: *error-message*; *action*

Description The chassis process (chassisd) tried to bring the indicated component (field-replaceable unit, or FRU) online, but the attempt failed in the indicated way. As a result, the chassisd process performed the indicated action.

Type Event: This message reports an event, not an error

Severity error

CHASSISD_FRU_UNRESPONSIVE_RETRY

System Log Message Attempt *count* to power on *fru-name fru-slot* timed out; restarted it

Description The chassis process (chassisd) tried the indicated number of times to bring the indicated component (field-replaceable unit, or FRU) online, but the attempts failed. In another attempt to bring the FRU online, the chassisd process issued the restart command for the FRU.

Type Event: This message reports an event, not an error

Severity error

CHASSISD_FRU_UNSUPPORTED

System Log Message chassisd invalidated support for *fru-name fru-slot*

Description The chassis process (chassisd) invalidated support for the indicated component (field-replaceable unit, or FRU) during initialization.

Type Error: An error occurred

Severity warning

CHASSISD_FRU_VERSION_MISMATCH

System Log Message *component* version mismatch for *fru-name* -- expected *expected-value*, got *received-value*

Description The chassis process (chassisd) verifies that it supports the revision level or version of a component (field-replaceable unit, or FRU). The revision level for the indicated FRU was unsupported or otherwise invalid.

Type Event: This message reports an event, not an error

Severity error

Action Upgrade the FRU.

CHASSISD_GASIC_ID_ERROR

System Log Message Fchip: invalid SIB slot

Description A routine tried to determine the identifier for an application-specific integrated circuit (ASIC) on a Switch Interface Board (SIB). The attempt failed, because the supplied SIB slot number was invalid.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_GBUS_NOT_READY

System Log Message *function-name*: *fru-name* not ready for power up (RTIME_PWR_COND = 0x*value*)

Description The GBUS was not ready when the chassis process (chassisd) first tried to power it on, and the power-up operation timed out.

Type Error: An error occurred

Severity error

Cause The probable cause is hardware error.

Action Contact your technical support representative.

CHASSISD_GBUS_READBACK_ERROR

System Log Message Readback error from GBUS for *fru-name fru-slot* ([0x*gbus-address*, 0x*gbus-registers*] -> 0x*return-value*)

Description There was an error when the chassis process (chassisd) tried to read back information from the GBUS on the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Cause The probable cause is hardware error.

Action Contact your technical support representative.

CHASSISD_GBUS_RESET_EVENT

System Log Message *fru-name#fru-slot - command*

Description The chassis process (chassisd) reset the GBUS for the indicated component (field-replaceable unit, or FRU). This is a normal part of startup.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_GBUS_SANITY_ERROR

System Log Message *function-name*: *fru-name fru-slot* -- management bus failed sanity test

Description The chassis process (chassisd) checks its management GBUS with a set of test operations when it is started. The tests failed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_GENERIC_ERROR

System Log Message *function-name*: *error-message*

Description The chassis process (chassisd) detected the indicated error.

Type Error: An error occurred

Severity error

Action Perform any corrective actions mentioned in the error message.

CHASSISD_GENERIC_WARNING

System Log Message *function-name*: *error-message*

Description The chassis process (chassisd) generated the indicated warning message.

Type Error: An error occurred

Severity notice

CHASSISD_GETTIMEOFDAY

System Log Message Unexpected error from gettimeofday: *error-code -- error-message*

Description The chassis process (chassisd) could not obtain the time of day because of the indicated error.

Type Error: An error occurred

Severity warning

CHASSISD_GRES_UNSUPP_INTERFACE

System Log Message Unable to enable graceful Routing Engine switchover; interface *interface-name* does not support it

Description The chassis process (chassisd) could not enable graceful Routing Engine switchover because the indicated interface does not support it.

Type Error: An error occurred

Severity error

CHASSISD_GRES_UNSUPP_PIC

System Log Message Unable to enable graceful Routing Engine switchover; PIC does not support it

Description The chassis process (chassisd) could not enable graceful Routing Engine switchover because an installed Physical Interface Card (PIC) does not support it.

Type Error: An error occurred

Severity error

CHASSISD_HIGH_TEMP_CONDITION

System Log Message Chassis temperature over *temperature* degrees C (*message*)

Description The temperature of one or more components (field-replaceable units, or FRUs) exceeded the indicated temperature, which is the lower of two thresholds. The fans (and impellers, if applicable) were in the indicated state. The chassis process (chassisd) increased the speed of all functioning fans and impellers to full speed.

Type Event: This message reports an event, not an error

Severity warning

Action Increase cooling in the area around the chassis.

CHASSISD_HOST_TEMP_READ

System Log Message Error reading host temperature sensor

Description The chassis process (chassisd) could not read the temperature sensors on the routing platform.

Type Error: An error occurred

Severity notice

CHASSISD_HSR_CONFIG_READ_ERROR

System Log Message *function-name*: unable to read configuration for HSR *identifier*

Description The indicated function could not read the configuration for the indicated high-speed receiver (HSR).

Type Error: An error occurred

Severity error

CHASSISD_HSR_CONFIG_WRITE_ERROR

System Log Message *function-name*: unable to write configuration for HSR *identifier*

Description The indicated routine could not write to the configuration for the indicated high-speed receiver (HSR).

Type Error: An error occurred

Severity error

CHASSISD_HSR_ELEMENTS_ERROR

System Log Message Provided number of HSR elements (*count*) was invalid

Description The indicated routine for processing a certain number of high-speed receiver (HSR) elements failed, because the supplied number of elements was invalid.

Type Error: An error occurred

Severity error

CHASSISD_HSR_FIFO_ERROR

System Log Message *function-name*: FIFO read failed for HSR *identifier*

Description A first in, first out (FIFO) read error occurred during execution of the indicated routine on the indicated high-speed receiver (HSR).

Type Error: An error occurred

Severity error

CHASSISD_I2CS_READBACK_ERROR

System Log Message Readback error from I2C slave for *fru-name fru-slot* ([0x*i2cs-address*, 0x*offset*] -> 0x*error-code*)

Description The chassis process (chassisd) could not read back information from the I2C slave (I2CS) about the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Cause The probable cause is hardware error.

Action Contact your technical support representative.

CHASSISD_I2C_BAD_IDEEPROM_FORMAT

System Log Message Invalid IDEEPROM format for *fru-name*

Description The chassis process (chassisd) determined that the ID EEPROM format specified for the indicated type of hardware component (field-replaceable unit, or FRU) is not valid for it.

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

CHASSISD_I2C_FIC_PRESENCE_READ

System Log Message *function-name*: *fru-name* unable to get presence masks (*error-message*)

Description The chassis process (chassisd) could not read I2C data with presence information about the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_I2C_GENERIC_ERROR

System Log Message *function-name*: *error-message*

Description The indicated error occurred during an I2C access library operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_I2C_INVALID_ASSEMBLY_ID

System Log Message '0x*assembly-id*' is invalid value for *fru-name* assembly ID

Description The assembly ID for the indicated component (field-replaceable unit, or FRU) was not valid for its type.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_I2C_IOCTL_FAILURE

System Log Message *function-name*: *operation* ioctl failure for group *group-id* at address 0x*address* (errno *error-code*)

Description The chassis process (chassisd) could not perform the indicated ioctl() operation on the I2C data for the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_I2C_IO_FAILURE

System Log Message *function-name*: *fru-name operation* failed for group *group-id* at address 0x*address*

Description The chassis process (chassisd) could not perform the indicated I/O operation on the I2C data for the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_I2C_MIDPLANE_CORRUPT

System Log Message Corruption on midplane ID EEPROM (ID: 0x*assembly-id*, MAC address: 0x*mac-address*, 0x*version*)

Description The chassis process (chassisd) found corrupted information when it tried to verify the parameters of the midplane's I2C ID EEPROM.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_I2C_RANGE_ERROR

System Log Message *function-name*: requested offset was out of range (offset *offset* + nbytes *count* > 256)

Description The indicated offset, which is greater than 256, was specified in a read request for an I2C device.

Type Error: An error occurred

Severity error

Cause No I2C device uses or has storage above an offset of 256.

Action Contact your technical support representative.

CHASSISD_I2C_READ_ERROR

System Log Message *function-name*: read error for group *group-id* at address 0x*address*, offset *offset*

Description The chassis process (chassisd) could not read I2C data from the indicated device.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_I2C_WRITE_ERROR

System Log Message *function-name*: write error for group *group-id* at address 0x*address*, offset *offset*

Description The chassis process (chassisd) could not write I2C data to the indicated device.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IDEEPROM_READ_ERROR

System Log Message Unable to read *fru-name* ID EEPROM

Description The chassis process (chassisd) could not read the I2C ID EEPROM of the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IFDEV_CREATE_FAILURE

System Log Message *function-name*: unable to create interface device for *interface-name* (*error-message*)

Description The chassis process (chassisd) creates initial interface devices for newly installed Physical Interface Cards (PICs) and pseudodevices. It could not create a device for the indicated PIC or pseudodevice.

Type Error: An error occurred

Severity error

Cause Necessary resources might have been unavailable.

Action Contact your technical support representative.

CHASSISD_IFDEV_CREATE_NOTICE

System Log Message *function-name*: created *device-name* for *interface-name*

Description The chassis process (chassisd) created the initial interface device for the indicated newly installed Physical Interface Card (PIC) or pseudodevice.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_IFDEV_DETACH_ALL_PSEUDO

System Log Message ifdev_detach(pseudo devices: all)

Description The chassis process (chassisd) detached the interface devices for all pseudodevices.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_IFDEV_DETACH_FPC

System Log Message ifdev_detach(*fpc-slot*)

Description The chassis process (chassisd) detached the interface devices for all Physical Interface Cards (PICs) installed in the indicated Flexible PIC Concentrator (FPC).

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_IFDEV_DETACH_PIC

System Log Message ifdev_detach_pic(*fpc-slot*/*pic-slot*)

Description The chassis process (chassisd) detached the interface devices for the indicated Physical Interface Card (PIC).

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_IFDEV_DETACH_PSEUDO

System Log Message ifdev_detach(pseudo devices: porttype *port-type*, sdev = *sdev-number*, edev = *edev-number*)

Description The chassis process (chassisd) detached the interface devices for the indicated pseudodevices.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_IFDEV_DETACH_TLV_ERROR

System Log Message ifdev_detach: rtslib_ifdm_change_tlvs failed for slot *fpc-slot* dev idx *device-id error-message*

Description The chassis process (chassisd) asked the kernel to remove the indicated interface from the kernel interface table. The request failed.

Type Error: An error occurred

Severity error

CHASSISD_IFDEV_GETBYNAME_NOTICE

System Log Message *function-name*: ifdm get_by_name failed for *interface-type* interface device *interface-name* (*error-message*)

Description The chassis process (chassisd) failed to find the indicated interface device, even though it just created it.

Type Event: This message reports an event, not an error

Severity warning

Cause There was a problem with interface state creation.

Action Contact your technical support representative.

CHASSISD_IFDEV_GET_BY_INDEX_FAIL

System Log Message *function-name*: rtslib_ifdm_get_by_index failed: *error-code - error-message*

Description The chassis process (chassisd) could not obtain information about an interface device.

Type Error: An error occurred

Severity error

CHASSISD_IFDEV_GET_BY_NAME_FAIL

System Log Message Unable to retrieve information for interface device *interface-name*: *error-message*

Description The chassis process (chassisd) could not obtain information about the indicated interface device.

Type Error: An error occurred

Severity error

CHASSISD_IFDEV_NO_MEMORY

System Log Message *function-name*: unable to allocate memory for *interface-type* interface

Description The chassis process (chassisd) could not allocate memory when creating an interface device for the indicated interface type.

Type Error: An error occurred

Severity error

Cause Resources on the system are extremely limited.

Action Eliminate the resource limitations and restart the Physical Interface Card (PIC) that houses the interface for which the interface device could not be created.

CHASSISD_IFDEV_RETRY_NOTICE

System Log Message *function-name*: attempt *count* to add interface device *interface-name* failed (*error-message*)

Description The chassis process (chassisd) tried the indicated number of times to create the indicated interface device, but the attempts failed. After generating this message, the chassisd process waited a while for resources to free up and tried again.

Type Event: This message reports an event, not an error

Severity warning

Cause Necessary resources might have been unavailable. They should become available soon.

CHASSISD_IFDEV_RTSLIB_FAILURE

System Log Message *function-name*: *library-function-name* failed (*error-message*)

Description The chassis process (chassisd) could not create an interface device because an error occurred during the indicated call to the routing socket library.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IOCTL_FAILURE

System Log Message *function-name*: *reason* for *fru-name* (*error-message*)

Description The chassis process (chassisd) could not perform the indicated ioctl() operation on the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_ANNOUNCE_TIMEOUT

System Log Message *function-name*: no ack received from *fru-type* for *fru-name fru-slot* state change (0x*sent-mask*, acks 0x*ack-mask*)

Description The chassis process (chassisd) notified the indicated components (field-replaceable units, or FRUs) that the component in the indicated slot was changing state. It did not receive the expected acknowledgment.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_CONNECTION_DROPPED

System Log Message Dropped IPC connection for *fru-name fru-slot*

Description The chassis process (chassisd) dropped its interprocess communication (IPC) connection to the indicated component (field-replaceable unit, or FRU).

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_IPC_DAEMON_WRITE_ERROR

System Log Message pipe_write failure for *connection-id*; connection error: *error-message* (errno *error-code*)

Description The chassis process (chassisd) could not write to a socket, because of the indicated error. The socket is for a connection to another process that runs on the Routing Engine and helps manage the chassis.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_ERROR

System Log Message *function-name*: *error-message*

Description An error occurred when the chassis process (chassisd) received an interprocess communication (IPC) message.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_FLUSH_ERROR

System Log Message *function-name*: flush operation failed for *fru-name fru-slot*

Description The chassis process (chassisd) could not write to a socket that it was using to communicate with the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

CHASSISD_IPC_MSG_DROPPED

System Log Message Dropping message from connection queue: type = *message-type*, subtype = *message-subtype*

Description The chassis process (chassisd) dropped an interprocess communication (IPC) message because the message queue had already reached maximum capacity.

Type Error: An error occurred

Severity error

Cause The connection to a component (field-replaceable unit, or FRU) no longer exists, so the chassisd process cannot send all messages immediately as it usually does.

Action Contact your technical support representative.

CHASSISD_IPC_MSG_ERROR

System Log Message *function-name*: error code *error-code*, type *message-type*, subtype *message-subtype*, opcode *message-opcode*

Description The chassis process (chassisd) detected an error in an interprocess communication (IPC) message with the indicated characteristics.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_MSG_FRU_NOT_FOUND

System Log Message *function-name*: unable to locate FRU for message with type *message-type*, subtype *message-subtype*, opcode *message-opcode*

Description The chassis process (chassisd) could not locate a component (field-replaceable unit, or FRU) to handle the interprocess communication (IPC) message with the indicated characteristics that it received. The message was ignored.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_MSG_QFULL_ERROR

System Log Message Dropping message from connection queue: type = *message-type*, subtype = *message-subtype*

Description The chassis process (chassisd) had to discard a message because the queue of messages waiting for a connection was already full.

Type Error: An error occurred

Severity error

CHASSISD_IPC_MSG_UNHANDLED

System Log Message *function-name*: unable to handle *fru-name* message with type *message-type*, subtype *message-subtype*, length *length*, opcode *message-opcode*, error *error-code*

Description The chassis process (chassisd) received an interprocess communication (IPC) message about the indicated FRU. The message had the indicated characteristics. The chassisd process could not handle the message.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_UNEXPECTED_MSG

System Log Message *function-name*: invalid message received: *message* (message type *message-type*, subtype *message-subtype*)

Description The chassis process (chassisd) received a unexpected message with the indicated characteristics.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_IPC_UNEXPECTED_RECV

System Log Message Received unexpected message from *connection-id*: type = *message-type*, subtype = *message-subtype*

Description The chassis process (chassisd) received an unexpected message from a peer connection.

Type Error: An error occurred

Severity error

CHASSISD_IPC_WRITE_ERROR

System Log Message *function-name*: pipe_write failure for SCC connection with error *error-code* (*error-message*)

Description A line-card chassis in a routing matrix attempted to send data to the TX Matrix platform (switch-card chassis, or SCC) over a pipe. The attempt failed with the indicated error.

Type Error: An error occurred

Severity warning

CHASSISD_IPC_WRITE_ERR_NO_PIPE

System Log Message FRU has no connection pipe *function-name fru-name*

Description The chassis process (chassisd) could not send a message to the indicated component (field-replaceable unit, or FRU) because the interprocess communication (IPC) pipe to the FRU no longer existed.

Type Error: An error occurred

Severity warning

CHASSISD_IPC_WRITE_ERR_NULL_ARGS

System Log Message FRU has no connection arguments *function-name fru-name*

Description The chassis process (chassisd) could not send a message to the indicated component (field-replaceable unit, or FRU) because one or more required parameters had a null value.

Type Error: An error occurred

Severity warning

CHASSISD_ISSU_BLOB_ERROR

System Log Message *fru-name*: *error-message*

Description The chassisd process (chassisd) detected the indicated error while handling blobs (opaque information) for the indicated field replaceable unit (fru). The blobs are used by the fru to store state information across in service software upgrade(issu) reboot.

Type Error: An error occurred

Severity notice

CHASSISD_ISSU_DAEMON_ERROR

System Log Message Daemon [*process-name*] state: < *state* > error: < *error-message* >

Description The chassisd process (chassisd) encountered the indicated error in the indicated in service software upgrade (issu) state for the indicated daemon.

Type Error: An error occurred

Severity notice

CHASSISD_ISSU_ERROR

System Log Message *action error-code*(*error-message*)

Description The chassisd process (chassisd) encountered the indicated error for the indicated in service software upgrade process (issu) action.

Type Error: An error occurred

Severity notice

CHASSISD_ISSU_FRU_ERROR

System Log Message *fru-name*: state:[*state*] *error-message*

Description The chassisd process (chassisd) encoutered the indicated error during the in service software upgrade for the indicated field replaceable unit (fru).

Type Error: An error occurred

Severity notice

CHASSISD_ISSU_FRU_IPC_ERROR

System Log Message *fru-name*: state:[*state*] error:[*message*] reason:[*error-message*]

Description The chassisd process (chassisd) detected the indicated error for the indicated field replaceable unit (fru) during in service software upgrade (issu).

Type Error: An error occurred

Severity notice

CHASSISD_JTREE_ERROR

System Log Message jtree terminate operation returned *error-code*

Description The chassis process (chassisd) received the indicated error when executing the JUNOS system call that terminates the jtree.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_LCC_RELEASE_MASTERSHIP

System Log Message Backup Routing Engine became master, because JUNOS version of former master did not match SCC master

Description The chassis process (chassisd) running on the master Routing Engine on a T640 routing node (line-card chassis, or LCC, in a routing matrix) relinquished mastership to the backup Routing Engine in the LCC.

Type Event: This message reports an event, not an error

Severity notice

Cause The version of the JUNOS software on the master Routing Engine did not match the version on the TX Matrix platform's master Routing Engine. The version on the backup Routing Engine did match the TX Matrix platform.

CHASSISD_LOST_MASTERSHIP

System Log Message Routing Engine lost mastership; exiting

Description The chassis process (chassisd) running on the master Routing Engine exited, because mastership switched to the other Routing Engine.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_MAC_ADDRESS_AE_ERROR

System Log Message chassisd MAC address allocation error for ae*device-id*

Description The chassis process (chassisd) could not obtain a media access control (MAC) address for the indicated aggregated Ethernet interface because of an internal error.

Type Error: An error occurred

Severity error

CHASSISD_MAC_ADDRESS_ERROR

System Log Message chassisd MAC address allocation exceed error for FPC *fpc-slot*, PIC *pic-slot*, port *port*

Description The chassis process (chassisd) could not obtain a media access control (MAC) address for the indicated interface because of an internal error.

Type Error: An error occurred

Severity error

CHASSISD_MAC_ADDRESS_FABRIC_ERR

System Log Message Unable to allocate MAC address for fabric interface *device-id*

Description The chassis process (chassisd) could not obtain a media access control (MAC) address for the indicated fabric interface because of an internal error.

Type Error: An error occurred

Severity error

CHASSISD_MAC_ADDRESS_IRB_ERROR

System Log Message chassisd MAC address allocation error for IRB

Description The chassis process (chassisd) could not obtain a media access control (MAC) address for an integrated routing and bridging interface because of an internal error.

Type Error: An error occurred

Severity error

CHASSISD_MAC_ADDRESS_VLAN_ERROR

System Log Message chassisd MAC address allocation error for VLAN

Description The chassis process (chassisd) could not obtain a media access control (MAC) address for a vlan interface because of an internal error.

Type Error: An error occurred

Severity error

CHASSISD_MAC_DEFAULT

System Log Message Using default MAC address base

Description The chassis process (chassisd) used the default base media access control (MAC) address.

Type Event: This message reports an event, not an error

Severity info

CHASSISD_MALLOC_FAILURE

System Log Message *function-name*: chassisd malloc failed, aborting

Description The chassis process (chassisd) could not allocate memory. The chassisd process tried to continue functioning, but the lack of memory usually causes the process to fail. An administrator needs to restart it at some point.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_MASTER_PCG_REMOVED

System Log Message Master PCG (slot *pcg-slot*) removed; powering down Packet Forwarding Engine complex

Description The master Packet Forwarding Engine Clock Generator (PCG) was removed. The PCG provides the system clock for all application-specific integrated circuits (ASICs) in the routing platform, so packet forwarding halts until the Packet Forwarding Engine is restarted and a PCG is functioning as master.

Type Error: An error occurred

Severity critical

CHASSISD_MASTER_SCG_REMOVED

System Log Message Master SCG (slot *fru-slot*) removed; powering it down

Description The master SONET Clock Generator (SCG) was removed. The SCG provides the clock for SONET/SDH interface timing, so those interfaces might drop packets and experience other errors until a new clock source is established.

Type Error: An error occurred

Severity critical

CHASSISD_MBUS_ERROR

System Log Message *fru-name fru-slot*: management bus failed sanity test

Description Startup tests on the indicated FRU's management bus failed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_MCHASSIS_SWITCH_WARNING

System Log Message CB settings on *chassis-type old-index* changed: switch is now '*value*', chassis index is now 0x*new-index*

Description A toggle switch on the back of the Control Board on each platform in a routing matrix is set to 'M' (multichassis) on the T640 routing nodes and to 'S' (single-chassis) on the TX Matrix platform. On a T640 routing node, the adjacent dial is set to the node's index number in the routing matrix (0 through 3); on the TX Matrix platform it is set to 0. The setting of the toggle switch, the dial, or both, changed to the indicated values on the indicated platform. The new settings take effect when the routing matrix next reboots.

Type Event: This message reports an event, not an error

Severity warning

Action If the changes were accidental, return the toggle and dial to the correct settings before the next reboot. If the changes were intended, disconnect and move the cables on the TX Matrix platform Switch Interface Board (SIB) to the row that corresponds to the T640 routing node's new index number.

CHASSISD_MCS_INTR_ERROR

System Log Message Received SIGUSR2 without any interrupts pending

Description The chassis process (chassisd) received the indicated interrupt signal. The signal normally indicates that an event on the Miscellaneous Control Subsystem (MCS) requires servicing. However, the chassisd process did not find such an event pending. This error does not usually cause component failure.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_MGR_CONNECT

System Log Message *function-name* evSelectFD: initial pipe create aborted (errno *error-code*)

Description The chassis process (chassisd) could not to open a pipe for interprocess communication (IPC) to a component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_MULTILINK_BUNDLES_ERROR

System Log Message Unable to set multilink Frame Relay UNI NNI bundles for PIC *pic-slot* in FPC *fpc-slot*

Description The chassis process (chassisd) could not create multilink Frame Relay user-to-network interface and network-to-network interface (MLFR UNI NNI [FRF.16]) bundles for the indicated Physical Interface Card (PIC).

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

CHASSISD_NO_PCGS

System Log Message No PCG *status*

Description The chassis process (chassisd) could not find an operational Packet Forwarding Engine Clock Generator (PCG). Packet forwarding is halted until a PCG becomes operational.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_NO_SCGS

System Log Message No SCG *state*

Description The chassis process (chassisd) could not find an operational SONET Clock Generator (SCG). To continue functioning correctly, SONET/SDH interfaces that use an SCG as their clock source must find another source.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_OFFLINE_NOTICE

System Log Message Routing Engine offline: *message*

Description The chassis process (chassisd) took the Routing Engine offline.

Type Event: This message reports an event, not an error

Severity critical

CHASSISD_OID_GEN_FAILED

System Log Message Unable to generate OID: *oid* (*error-message*)

Description The chassis process (chassisd) could not generate an object identifier (OID) for the indicated object.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_OVER_TEMP_CONDITION

System Log Message Chassis temperature over *temperature* degrees C (*message*); routing platform will shutdown in *duration* seconds if condition persists

Description The temperature of one or more components (field-replaceable units, or FRUs) exceeded the indicated temperature, which is the upper of two thresholds. The fans (and impellers, if applicable) were in the indicated state. If the temperature does not go below the threshold within four minutes after the chassis process (chassisd) detects this condition, the chassisd process shuts down the routing platform. When this message was logged, the indicated number of seconds remained before shutdown.

Type Error: An error occurred

Severity error

Action Increase cooling in the area around the chassis.

CHASSISD_OVER_TEMP_SHUTDOWN_TIME

System Log Message Chassis temperature above *temperature* degrees C *description* (> *duration* seconds); powering down all FRUs

Description The chassis process (chassisd) shut down the routing platform because the temperature of one or more components exceeded the indicated threshold temperature for the indicated amount of time. Continued operation at the excessive temperature could damage the routing platform.

Type Error: An error occurred

Severity critical

Action Increase cooling in the area around the chassis.

CHASSISD_PARSE_COMPLETE

System Log Message Using new configuration

Description The chassis process (chassisd) successfully parsed its configuration file.

Type Event: This message reports an event, not an error

Severity info

CHASSISD_PCI_ERROR

System Log Message *function-name*: *error-message*

Description While performing an operation on the PCI bus, the chassis process (chassisd) encountered the indicated error.

Type Error: An error occurred

Severity error

Cause A software or a hardware problem occurred.

Action Contact your technical support representative.

CHASSISD_PEER_UNCONNECTED

System Log Message *function-name*: peer not connected

Description The chassis process (chassisd) processed a packet for a peer with an invalid or missing connection.

Type Event: This message reports an event, not an error

Severity error

Cause In most cases, this error is caused by peers transitioning up and down unexpectedly. The error is usually transient and nonfatal.

CHASSISD_PEM_BREAKER_TRIP

System Log Message Circuit breaker tripped for power supply *pem-slot*

Description The circuit breaker was tripped for the indicated power entry module (PEM).

Type Event: This message reports an event, not an error

Severity warning

Action Turn on the affected PEM manually.

CHASSISD_PEM_INPUT_BAD

System Log Message *error-message* for power supply *pem-slot* (status bits: 0x*status-code*); check circuit breaker

Description The chassis process (chassisd) detected the indicated error condition for the indicated power entry module (PEM).

Type Event: This message reports an event, not an error

Severity warning

Action Check the status of the circuit breaker and the input connections.

CHASSISD_PEM_NOT_SUFFICIENT

System Log Message Unable to power up FPC *fpc-slot*, because no three-input 240-A power supply is installed

Description On the T1600 router, the T1600-FPC4 ES Flexible PIC Concentrator (FPC) requires that at least one three-input 240-A power supply be installed. The chassis process (chassisd) did not power on the T1600-FPC4 ES in the indicated slot because the required power supply is not installed.

Type Error: An error occurred

Severity error

Action Install at least one three-input 240-A power supply.

CHASSISD_PEM_OVERLOAD

System Log Message Overload condition for power supply *pem-slot* (status bits: 0x*status-code*);

Description The indicated power entry module (PEM) reported an output voltage overload condition.

Type Event: This message reports an event, not an error

Severity warning

Cause There might have been excessive load on the PEM.

CHASSISD_PEM_TEMPERATURE

System Log Message Temperature check bit set for power supply *pem-slot*; airflow might be inadequate

Description The chassis process (chassisd) detected that the 'temperature check bit' was set in the status bit mask for the indicated power entry module (PEM).

Type Event: This message reports an event, not an error

Severity warning

Cause The PEM might have exceeded its temperature threshold, possibly because the airflow through it was inadequate.

CHASSISD_PEM_VOLTAGE

System Log Message Power supply *pem-slot* reports problem; check output voltage

Description The indicated power entry module (PEM) reported a problem with its output voltage.

Type Event: This message reports an event, not an error

Severity warning

Cause There might have been excessive load on the PEM.

CHASSISD_PFE_SUPPORT_ERROR

System Log Message *function-name*: *fpc-slot*

Description The chassis process (chassisd) detected an FPC in an unsupported slot with six-slot configuration set.

Type Error: An error occurred

Severity error

CHASSISD_PIC_CMD_GIVEUP

System Log Message *function-name*: attempt *fpc-slot* to bring PIC *pic-slot* in FPC *count* online timed out; stopped trying

Description The chassis process (chassisd) tried the indicated number of times to bring the indicated Physical Interface Card (PIC) online, but stopped trying after all attempts failed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_PIC_CMD_TIMEOUT

System Log Message *function-name*: attempt to bring PIC *pic-slot* in FPC *fpc-slot* online timed out

Description The chassis process (chassisd) tried to bring the indicated Physical Interface Card (PIC) online. The attempt took longer than the standard time allotted for that operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_PIC_CONFIG_ERROR

System Log Message Unable to create interface devices during attachment of PIC *pic-slot* in FPC *fpc-slot*: graceful switchover not supported

Description The chassis process (chassisd) did not create an interface device for the indicated Physical Interface Card (PIC), because graceful switchover was enabled but is not supported in combination with that PIC type. A PIC must have an interface device to come online, so it remained offline.

Type Error: An error occurred

Severity error

Action Remove the PIC or upgrade the JUNOS software.

CHASSISD_PIC_HWERROR

System Log Message PIC *pic-slot* in FPC *fpc-slot* (PIC type *pic-type*, version *version*) had hardware error

Description The indicated Physical Interface Card (PIC) experienced a hardware error. The chassis process (chassisd) did not bring the PIC online.

Type Event: This message reports an event, not an error

Severity warning

Action Contact your technical support representative.

CHASSISD_PIC_OFFLINE_NOTICE

System Log Message Taking PIC *pic-slot* in FPC *fpc-slot* offline: *reason*

Description The chassis process (chassisd) took the indicated Physical Interface Card (PIC) offline, for the indicated reason.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_PIC_OID_GEN_FAILED

System Log Message Unable to generate OID for PIC: *pic-name* (*error-message*)

Description The chassis process (chassisd) could not generate an object identifier (OID) for the indicated Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_PIC_OID_UNKNOWN

System Log Message Unable to find OID for PIC: *i2c-id*

Description The chassis process (chassisd) could not determine the object identifier (OID) for the Physical Interface Card (PIC) with the indicated identifier.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_PIC_RESET_ON_SWITCHOVER

System Log Message PIC *pic-slot* in FPC *fpc-slot* (type *pic-type*, version *version*) will be reset on switchover

Description The chassis process (chassisd) noted that the Physical Interface Card (PIC) with the indicated characteristics needs to be reset when a graceful switchover occurs.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_PIC_SPEED_INVALID

System Log Message Set speed for so-*fpc-slot*/*pic-slot*/*port* to *default-value* because configured value *current-value* is invalid

Description The chassis process (chassisd) set the speed for the indicated Physical Interface Card (PIC) to the indicated value, because the configured value is either higher than the maximum valid value or lower than the minimum valid value.

Type Error: An error occurred

Severity error

Action Reconfigure the PIC with a valid speed.

CHASSISD_PIC_VERSION_ERROR

System Log Message Hardware version (*pic-slot*) of PIC *fpc-slot* in FPC *pic-type* (PIC type *version*) is not supported

Description The chassis process (chassisd) did not bring the indicated Physical Interface Card (PIC) online, because its hardware version is not supported.

Type Error: An error occurred

Severity warning

Cause The PIC requires a hardware upgrade.

Action Contact your technical support representative.

CHASSISD_PIDFILE_OPEN

System Log Message Unable to open PID file '*filename*': errno *error-code*

Description The chassis process (chassisd) could not open the file where it stores its process ID (PID).

Type Error: An error occurred

Severity error

Cause The chassisd process might have detected that another chassisd process was running and tried to read the file so that it could use the PID recorded there when terminating the other process.

CHASSISD_PIPE_WRITE_ERROR

System Log Message Pipe write error: *error-message*

Description The chassis process (chassisd) experienced a fatal error while writing to a pipe.

Type Error: An error occurred

Severity error

Cause There was no reader for the pipe.

CHASSISD_POWER_CHECK

System Log Message *fru-name fru-slot* not powering up

Description The chassis process (chassisd) could not power up the indicated component (field-replaceable unit, or FRU), because the FRU did not respond.

Type Error: An error occurred

Severity error

CHASSISD_POWER_EVENT

System Log Message Unable to turn off power to *fru-name fru-slot*; a stand-alone test jumper might be installed

Description The chassis process (chassisd) could not turn off power to the indicated component (field-replaceable unit, or FRU).

Type Event: This message reports an event, not an error

Severity warning

Cause A common reason is that a standalone test jumper is installed.

CHASSISD_POWER_RATINGS_EXCEEDED

System Log Message PIM/module in slot *fru-slot* left offline to avoid exceeding chassis power ratings

Description The chassis process (chassisd) did not bring online the component (field-replaceable unit, or FRU) in the indicated slot, because doing so causes the total power demand of components in the chassis to exceed the chassis' power ratings. On a J-series Services Router, the component is a Physical Interface Module (PIM) or other module that installs in a PIM slot.

Type Error: An error occurred

Severity error

CHASSISD_PSD_RELEASE_MASTERSHIP

System Log Message Backup Routing Engine became master, because JUNOS version of former master did not match RSD master

Description The chassis process (chassisd) running on the master Routing Engine on a System-Domain routing node relinquished mastership to the backup Routing Engine in the PSD.

Type Event: This message reports an event, not an error

Severity notice

Cause The version of the JUNOS software on the master Routing Engine did not match the version on the RSD platform's master Routing Engine. The version on the backup Routing Engine did match the RSD platform.

CHASSISD_PSU_ERROR

System Log Message *error-message* power supply *pem-slot* (status bits: 0x*status-code*); status failure

Description The chassis process (chassisd) detected the indicated error condition for the indicated power supply unit (PSU).

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_PSU_FAN_FAIL

System Log Message Fan Fail for power supply *pem-slot*

Description PSU Fan fail bit is set in the status for the indicated power supply unit (PSU)

Type Error: An error occurred

Severity warning

CHASSISD_PSU_INPUT_BAD

System Log Message *error-message* power supply *pem-slot* (status bits: 0x*status-code*); Input failure

Description The chassis process (chassisd) detected the input voltage/warning fault condition for the indicated power supply unit (PSU).

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_PSU_OVERLOAD

System Log Message Overload condition for power supply *pem-slot* (status bits: 0x*status-code*);

Description The indicated power supply unit (PSU) reported an output voltage overload condition.

Type This message reports an event, not an error

Severity warning

Cause There might have been excessive load on the PSU.

CHASSISD_PSU_TEMPERATURE

System Log Message Temperature check bit set for power supply *pem-slot*; airflow might be inadequate

Description The chassis process (chassisd) detected that the 'temperature check bit' was set in the status bit mask for the indicated power supply unit (PSU).

Type Event: This message reports an event, not an error

Severity warning

Cause The PSU might have exceeded its temperature threshold, possibly because the airflow through it was inadequate.

CHASSISD_PSU_VOLTAGE

System Log Message Power supply *pem-slot* reports problem; check output voltage

Description The indicated power supply unit (PSU) reported a problem with its output voltage.

Type Event: This message reports an event, not an error

Severity warning

Cause There might have been excessive load on the PSU.

CHASSISD_RANGE_CHECK

System Log Message *function-name*: '0x*value*' is invalid value for *object-name* (out of range)

Description The indicated value was outside the valid range of values for the indicated object.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_RECONNECT_SUCCESSFUL

System Log Message Successfully reconnected on soft restart

Description The chassis process (chassisd) successfully reconnected with each Packet Forwarding Engine after a soft restart.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_RELEASE_MASTERSHIP

System Log Message Release mastership notification

Description The chassis process (chassisd) running on the master Routing Engine received a request to release mastership.

Type Event: This message reports an event, not an error

Severity info

Cause The Routing Engine was probably rebooting and graceful Routing Engine switchover is configured.

CHASSISD_RE_INIT_INVALID_RE_SLOT

System Log Message re_init: re *routing-engine-slot*, out of range

Description The chassis process (chassisd) could not initialize a Routing Engine because the slot number specified for it was invalid.

Type Error: An error occurred

Severity error

CHASSISD_RE_OVER_TEMP_CONDITION

System Log Message Routing Engine *routing-engine-slot* temperature (*temperature* C) over *threshold* degrees C

Description The temperature of the indicated Routing Engine exceeded the indicated temperature, which is the upper of two thresholds.

Type Error: An error occurred

Severity error

Action Increase cooling in the area around the chassis.

CHASSISD_RE_OVER_TEMP_SHUTDOWN

System Log Message Routing Engine *routing-engine-slot* temperature above *threshold* degrees C for too long; *action*

Description The chassis process (chassisd) performed the indicated action because the temperature of the indicated Routing Engine exceeded the maximum threshold for more than four minutes. Continued operation at the excessive temperature could damage routing platform components.

Type Error: An error occurred

Severity critical

Action Increase cooling in the area around the chassis.

CHASSISD_RE_OVER_TEMP_WARNING

System Log Message Routing Engine *routing-engine-slot* temperature (*temperature* C) over *threshold* degrees C, *component* will shutdown in *duration* seconds if condition persists

Description The temperature of the indicated Routing Engine exceeded the indicated temperature, which is the upper of two thresholds. If the temperature does not go below the threshold within four minutes after the chassis process (chassisd) detects this condition, the chassisd process shuts down the indicated component. When this message was logged, the indicated number of seconds remained before shutdown.

Type Error: An error occurred

Severity error

Action Increase cooling in the area around the chassis.

CHASSISD_RE_WARM_TEMP_CONDITION

System Log Message Routing Engine *routing-engine-slot* temperature (*temperature* C) is above warm temperature limit (*threshold* C)

Description The temperature of the indicated Routing Engine exceeded the indicated temperature, which is the lower of two thresholds.

Type Event: This message reports an event, not an error

Severity error

Action Increase cooling in the area around the chassis.

CHASSISD_ROOT_MOUNT_ERROR

System Log Message Unable to determine the mount point for root directory: *error-message*

Description The chassis process (chassisd) could not determine the mount point for the root file system.

Type Error: An error occurred

Severity error

CHASSISD_RTS_SEQ_ERROR

System Log Message ifmsg sequence gap *expected-value - received-value*

Description The chassis process (chassisd) received a routing socket message out of order.

Type Event: This message reports an event, not an error

Severity warning

Cause A routing socket message was lost because of excessive load or lack of memory.

CHASSISD_SBOARD_VERSION_MISMATCH

System Log Message Version mismatch: chassisd message version *expected-value fru-name* message version *received-value* local IPC version *local-ipc-version* remote IPC version *remote-ipc-version*

Description The chassis process (chassisd) verifies that it supports the revision level or version of a component (field-replaceable unit, or FRU). The revision level for the indicated FRU was unsupported or otherwise invalid.

Type Error: An error occurred

Severity error

Cause Either a previous software upgrade did not complete successfully, or the chassisd process or FRU did not restart after a successful software upgrade.

Action Upgrade the software and reboot the routing platform.

CHASSISD_SENSOR_RANGE_NOTICE

System Log Message *fru-name fru-slot* temperature is *temperature* degrees C, which is outside operating range

Description The temperature sensor on the indicated component (field-replaceable unit, or FRU) reported the indicated temperature, which is outside the acceptable operating range.

Type Event: This message reports an event, not an error

Severity warning

Cause Some sensors generate erroneous readings when a FRU starts up. When this happens, the chassis process (chassisd) rereads the sensor at a later time.

CHASSISD_SERIAL_ID

System Log Message Serial ID read error: *error-code -- error-message*

Description The chassis process (chassisd) could not obtain the Routing Engine's serial number from the kernel because of the indicated error.

Type Error: An error occurred

Severity warning

CHASSISD_SFM_MODE_ERROR

System Log Message *function-name*: *error-message*

Description The chassis process could not configure a requested operational mode for a Switching and Forwarding Module (SFM), for the indicated reason.

Type Error: An error occurred

Severity info

Cause Possible reasons include (a) the requested mode is available only with certain versions of an application-specific integrated circuit (ASIC) (b) not all SFMs are online as required by the requested mode (c) cross-connect mode cannot be configured if an OC-192c Physical Interface Card (PIC) is installed.

CHASSISD_SFM_NOT_ONLINE

System Log Message *function-name*: SFM *sfm-slot* not online

Description The indicated Switching and Forwarding Module (SFM) was offline.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_SHUTDOWN_NOTICE

System Log Message Shutdown reason: *reason*

Description Although the chassis process (chassisd) normally does not exit or shut down except when the Routing Engine reboots, it shut down for the indicated reason.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_SIGPIPE

System Log Message SIGPIPE received

Description The chassis process (chassisd) received a signal indicating that its attempt to write to a pipe failed because the reader (which could be another process or thread) did not exist.

Type Event: This message reports an event, not an error

Severity error

Cause The entity at the other end of the pipe exited or closed the connection.

CHASSISD_SMB_ERROR

System Log Message smb_read: fpga download not complete: val *return-value*, *action*

Description The system management bus (SMB) could not download field-programmable gate array (FPGA) information and returned the indicated status code. The chassis process (chassisd) took the indicated action.

Type Error: An error occurred

Severity error

CHASSISD_SMB_INVALID_PS

System Log Message *function-name*: invalid power supply status code (0x*status-code*)

Description The chassis process (chassisd) could not set the status (enabled or disabled) for a power supply, because it received the indicated power supply status code, which is invalid.

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

CHASSISD_SMB_IOCTL_FAILURE

System Log Message *function-name*: '*operation*' ioctl failed on system management bus (address 0x*memory-address*, cmd 0x*command*)

Description The indicated ioctl() operation failed at the indicated address on the system management bus (SMB).

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

CHASSISD_SMB_READ_FAILURE

System Log Message *function-name*: read() failed on system management bus (address 0x*memory-address*)

Description A read() operation failed at the indicated address on the system management bus (SMB).

Type Error: An error occurred

Severity critical

Action Contact your technical support representative.

CHASSISD_SNMP_TRAP1

System Log Message SNMP trap generated: *trap* (*argument1 value1*)

Description The chassisd process (chassisd) generated the indicated simple network management protocol (snmp) trap with the indicated value.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_SNMP_TRAP10

System Log Message SNMP trap generated: *trap* (*argument1 value1*, *argument2 value2*, *argument3 value3*, *argument4 value4*, *argument5 value5*, *argument6 value6*, *argument7 value7*, *argument8 value8*, *argument9 value9*, *argument10 value10*)

Description The chassis process (chassisd) generated a Simple Network Management Protocol (SNMP) trap with the ten indicated argument-value pairs.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_SNMP_TRAP6

System Log Message SNMP trap generated: *trap* (*argument1 value1*, *argument2 value2*, *argument3 value3*, *argument4 value4*, *argument5 value5*, *argument6 value6*)

Description The chassis process (chassisd) generated a Simple Network Management Protocol (SNMP) trap with the six indicated argument-value pairs.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_SNMP_TRAP7

System Log Message SNMP trap generated: *trap* (*argument1 value1*, *argument2 value2*, *argument3 value3*, *argument4 value4*, *argument5 value5*, *argument6 value6*, *argument7 value7*)

Description The chassis process (chassisd) generated a Simple Network Management Protocol (SNMP) trap with the seven indicated argument-value pairs.

Type Event: This message reports an event, not an error

Severity notice

CHASSISD_SPMB_RESTART

System Log Message SPMB *slot* restarted

Description The indicated Switch Processor Mezzanine Board (SPMB) restarted.

Type Event: This message reports an event, not an error

Severity info

CHASSISD_SPMB_RESTART_TIMEOUT

System Log Message Attempt *count* to restart SPMB *slot* timed out; *action*

Description The chassis process (chassisd) tried the indicated number of times to bring the indicated Switch Processor Mezzanine Board (SPMB) online. The chassisd process performed the indicated action as a result of the failure.

Type Event: This message reports an event, not an error

Severity error

CHASSISD_SSB_FAILOVERS

System Log Message *fru-name* failover occurred *count* times

Description The indicated packet-switching component or control board failed over to a redundant neighbor the indicated number of times, which exceeds the maximum limit.

Type Event: This message reports an event, not an error

Severity warning

Cause There is probably a system error.

Action Contact your technical support representative.

CHASSISD_STANDALONE_FPC_NOTICE

System Log Message chassisd running in standalone FPC mode *mode*

Description The chassis process (chassisd) was running in the indicated standalone Flexible PIC Concentrator (FPC) mode. This message was logged in case the administrator wants it to run in a different mode.

Type Event: This message reports an event, not an error

Severity warning

CHASSISD_SYSCTL_ERROR

System Log Message *function-name*: *sysctl-error* error from *sysctl-function-name*: *error-message* (errno *error-code*)

Description The chassis process (chassisd) received the indicated error from the indicated sysctl() operation.

Type Error: An error occurred

Severity error

CHASSISD_TEMP_HOT_NOTICE

System Log Message *fru-name* temperature of *temperature* degrees C is above limit (*threshold* degrees)

Description The temperature of the chassis, or of the indicated component (field-replaceable unit, or FRU), exceeded the lower of two thresholds. The chassis process (chassisd) increased the speed of all functioning fans (and impellers, if applicable) to full speed. If the temperature did not decrease below the threshold within 4 minutes after this message was logged, the chassisd process shut down the routing platform.

Type Event: This message reports an event, not an error

Severity error

Action Increase cooling in the area around the chassis.

CHASSISD_TEMP_SENSOR_FAILURE

System Log Message *function-name*: unable to read temperature sensor for *fru-name*

Description The temperature sensor for the indicated component (field-replaceable unit, or FRU) either did not respond to a request from the chassis process (chassisd) for a temperature reading or sent a value that is outside the normal operating range.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_TERM_SIGNAL

System Log Message Received SIGTERM request, shutting down

Description The chassis process (chassisd) received the SIGTERM signal, indicating that it should terminate. It began the procedure for clean shutdown and exit, but possibly restarted automatically after exiting.

Type Event: This message reports an event, not an error

Severity info

CHASSISD_TIMER_CLR_ERR

System Log Message *function-name*: *message*

Description The chassis process (chassisd) could not clear the state of the timer it had set to track the timeout period for an event.

Type Error: An error occurred

Severity error

CHASSISD_TIMER_ERR

System Log Message Unable to schedule timeout for *description*

Description The chassis process (chassisd) could not start a timer to track the timeout period for the indicated event. The seriousness of this error depends on the event.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_TIMER_VAL_ERR

System Log Message Null timer ID

Description The chassis process (chassisd) started a timer to track the timeout period for an event. The timer returned a null identifier, so the chassisd process could not clear the timer.

Type Error: An error occurred

Severity error

CHASSISD_UNEXPECTED_EXIT

System Log Message evMainLoop returned *return-value* (errno *error-code*)

Description The chassis process (chassisd) exited unexpectedly and reported the indicated error.

Type Error: An error occurred

Severity error

CHASSISD_UNEXPECTED_VALUE

System Log Message *function-name*: '*value*' is invalid value for *object-name*

Description The indicated value was specified for the indicated object in a message received by the chassis process (chassisd). The value is invalid for that type of object.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

CHASSISD_UNSUPPORTED_FPC

System Log Message FPC with I2C ID of 0x*i2c-id* is not supported

Description A Flexible PIC Concentrator (FPC) of the indicated type was installed in the routing platform. The software does not support that FPC type on this platform.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_UNSUPPORTED_MODEL

System Log Message Model *model* unsupported with this version of chassisd

Description The version of the chassis process (chassisd) software that is installed on the routing platform does not support this type of chassis.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

CHASSISD_UNSUPPORTED_PIC

System Log Message PIC *pic-slot* in FPC *fpc-slot* (type *pic-type*, version *version*) is not supported

Description The indicated Physical Interface Card (PIC) is either not supported on this routing platform or is not supported by the installed version of the chassis process (chassisd) software. The chassisd process did not bring the PIC online.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

CHASSISD_UNSUPPORTED_PIC_MODE

System Log Message Application mode *mode* is not supported for PIC *pic-slot* in FPC *fpc-slot*

Description The indicated Physical Interface Card (PIC) does not support the indicated application mode configured for it.

Type Event: This message reports an event, not an error

Severity warning

Action Check which application modes are supported for the PIC.

CHASSISD_UNSUPPORTED_SIB

System Log Message SIB with assembly ID *assembly-id* is not supported

Description The chassis process (chassisd) detected the presence of a new Switch Interface Board (SIB) with the indicated assembly ID. The SIB remains offline, because it is not a supported type.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_VERSION_MISMATCH

System Log Message Version mismatch: chassisd message version *expected-value fru-name fru-slot* message version *received-value* local IPC version *local-ipc-version* remote IPC version *remote-ipc-version*

Description As a component (field-replaceable unit, or FRU) comes online, the chassis process (chassisd) verifies that the FRU's revision level or version is supported. The revision level of the indicated FRU was unsupported or otherwise invalid.

Type Error: An error occurred

Severity error

Cause Either a previous software upgrade did not complete successfully, or the chassisd process or FRU did not restart after a successful software upgrade.

Action Upgrade the software and reboot the routing platform.

CHASSISD_VOLTAGE_READ_FAILED

System Log Message Unable to read voltage from *fru-name* (group *group-id*, address *address*, channel *voltage-channel*)

Description The chassis process (chassisd) could not read voltage data from the indicated component (field-replaceable unit, or FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

CHASSISD_VOLTAGE_SENSOR_INIT

System Log Message Unable to initialize voltage sensor for *fru-name* (group *group-id*, address *address*)

Description The chassis process (chassisd) could not initialize the voltage sensor for the indicated component (field-replaceable unit, for FRU).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

Chapter 16

CONTENT System Log Messages

This chapter describes messages with the CONTENT prefix. They are generated by the content filtering process (content).

CONTENT_FILTERING_BLOCKED

System Log Message Content Filtering: *argument* (*profile-name*) from *source-address* is *action* due to *reason*

Description The transaction is blocked due to content filtering setting

Type Event: This message reports an event, not an error

Severity info

Cause The transaction is in content filtering's block list

Action Check the transaction to make sure it is not a false positive

CONTENT_FILTERING_BLOCKED_MT

System Log Message Content Filtering: *argument* (*profile-name*) from *source-address* is *action* due to *reason*

Description The transaction is blocked due to content filtering setting

Type Event: This message reports an event, not an error

Severity info

Cause The transaction is in content filtering's block list

Action Check the transaction to make sure it is not a false positive

Chapter 17

COSD System Log Messages

This chapter describes messages with the COSD prefix. They are generated by the class-of-service (CoS) process (cosd), which enables the routing platform to provide different levels of service to applications based on packet classifications.

COSD_CHASSIS_SCHED_MAP_INVALID

System Log Message Chassis scheduler map incorrectly applied to interface *interface-name*: *error-message*

Description The class-of-service (CoS) process (cosd) did not apply a chassis scheduler map to the indicated interface, because the configuration used to apply the scheduler map was invalid.

Type Error: An error occurred

Severity error

Cause One possible cause is that the chassis scheduler map is applied to a specific interface. For most interface types, a scheduler map must be applied to all interfaces on the Physical Interface Card (PIC); therefore, a wildcard must be used to specify the interfaces. One exception to this rule is the Gigabit Ethernet IQ PIC.

Action Correct the configuration used to apply the chassis scheduler map to the interface.

COSD_CONF_OPEN_FAILURE

System Log Message Unable to open: *filename*, using default CoS forwarding classes, do 'commit full' in cli to avoid this message

Description The class-of-service (CoS) process (cosd) could not read configuration data.

Type Error: An error occurred

Severity error

Cause All of the following:mgd -I fails after upgrade (cosd.conf does not exist and is not created because of the mgd -I failure), the first commit is 'commit' and not 'commit full'(cosd.conf will not commit is 'commit' and not 'commit full'(cosd.conf will not automatically be created), [class-of-service forwarding-classes] does notexist(the file cosd.conf will not get exported with plain 'commit')

Action Do a 'commit full'

COSD_DB_OPEN_FAILED

System Log Message Unable to open configuration database: *error-message*

Description The class-of-service (CoS) process (cosd) could not read configuration data for the indicated reason.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

COSD_EXACT_RATE_UNSUPP_INTERFACE

System Log Message Unable to apply scheduler map *scheduler-map* to interface *interface-name* because it does not support exact-rate transmission

Description The class-of-service (CoS) process (cosd) did not apply the indicated scheduler map to the indicated interface, because a scheduler named in the scheduler map specifies exact transmission rate. The interface is housed on a type of Physical Interface Card (PIC) that does not support exact transmission rate, such as an IQ2 PIC. In terms of configuration, the 'exact' statement is included in the scheduler definition at the [edit class-of-service schedulers <scheduler-name> transmit-rate (<rate> | percent <percentage>)] hierarchy level. The scheduler is included in the scheduler map that is applied to the interface.

Type Error: An error occurred

Severity error

Action Remove the 'exact' statement from the scheduler in the scheduler map applied to the interface.

COSD_EXACT_RATE_UNSUPP_SESSION

System Log Message Unable to apply CoS to L2TP session *session-id*, because scheduler map *scheduler-map* specifies exact rate transmission

Description The class-of-service (CoS) process (cosd) did not apply CoS settings to the indicated Layer 2 Tunneling Protocol (L2TP) session, because the scheduler map specified by the RADIUS server for the session is configured for exact transmission rate. Exact transmission rate is not supported for L2TP sessions on the type of Physical Interface Card (PIC) that houses the interface, such as an IQ2 PIC. In terms of configuration, the 'exact' statement is included in a scheduler definition at the [edit class-of-service schedulers <scheduler-name> transmit-rate (<rate> | percent <percentage>)] hierarchy level. The scheduler is included in a scheduler map that is associated with a traffic control profile. The traffic control profile is named by an attribute in the RADIUS server's configuration file, which makes the profile apply to the session.

Type Error: An error occurred

Severity error

Action Remove the 'exact' statement from the scheduler in the scheduler map applied to the session.

COSD_FRAGMENTATION_MAP_CONFLICT

System Log Message Interface *compression-device* matches wildcard *wildcard-interface-name*, but fragmentation map *fragmentation-map* was not applied because interface is compression device for link interface *link-interface-name*

Description The indicated fragmentation map is normally applied to interfaces that match the indicated wildcard. The class-of-service (CoS) process (cosd) did not apply the fragmentation map to the indicated interface, even though it matches the wildcard, because the interface is acting as a compression device for the indicated link interface.

Type Error: An error occurred

Severity warning

Action Correct the configuration of the fragmentation map.

COSD_HIGH_PRIO_QUEUES_INTERFACE

System Log Message Unable to apply scheduler map *scheduler-map* to interface *interface-name*, because multiple schedulers in map have "high,""medium-high," or "strict-high" priority

Description The class-of-service (CoS) process (cosd) did not apply the indicated scheduler map to the indicated interface, because the map includes more than one scheduler that has high, medium-high, or strict-high priority. For interfaces that are housed by certain Physical Interface Cards (PICs), such as an IQ2 PIC, the scheduler map can include only one scheduler that specifies one of those three priority levels. In terms of configuration, the 'priority' statement at the [edit class-of-service schedulers <scheduler-name>] hierarchy level has the value 'high, ' 'medium-high, ' or 'strict-high' for more than one of the schedulers in the map.

Type Error: An error occurred

Severity error

Action Correct the configuration so that the scheduler map includes only one scheduler with high, medium-high, or strict-high priority.

COSD_HIGH_PRIO_QUEUES_SESSION

System Log Message Unable to apply CoS to L2TP session *session-id*, because multiple schedulers in scheduler map *scheduler-map* have "high,""medium-high," or "strict-high" priority

Description The class-of-service (CoS) process (cosd) did not apply CoS settings to the indicated Layer 2 Tunneling Protocol (L2TP) session, because the scheduler map specified by the RADIUS server for the session includes more than one scheduler that has high, medium-high, or strict-high priority. For interfaces that are housed by certain Physical Interface Cards (PICs), such as an IQ2 PIC, the scheduler map can include only one scheduler that specifies one of those three priority levels. In terms of configuration, the 'priority' statement at the [edit class-of-service schedulers <scheduler-name>] hierarchy level has the value 'high, ' 'medium-high, ' or 'strict-high' for more than one of the schedulers in the map. The map is associated with a traffic control profile

that is named by an attribute in the RADIUS server's configuration file, which makes the profile apply to the session.

Type Error: An error occurred

Severity error

Action Correct the configuration so that the scheduler map includes only one scheduler with high, medium-high, or strict-high priority.

COSD_HWDB_OPEN_FAILED

System Log Message Unable to open chassis hardware database: *error-message*

Description The class-of-service (CoS) process (cosd) encountered the indicated error while opening the chassis hardware database.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

COSD_IFD_OUTPUT_SHAPING_RATE_ERR

System Log Message Traffic shaping not supported on interface device *interface-name*

Description The class-of-service (CoS) process (cosd) did not apply the shaping rate that is configured for the indicated interface.

Type Error: An error occurred

Severity error

Cause Shaping rate is valid only for interfaces housed by IQ and IQ2 Physical Interface Cards (PICs), and the interface is on a different type of PIC.

Action Remove the shaping rate configuration from the interface.

COSD_INTERFACE_NO_MEDIA

System Log Message Unable to obtain media information for interface *interface-name*

Description The message sent by the kernel for the indicated interface did not include required media information.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

COSD_L2TP_COS_NOT_CONFIGURED

System Log Message Unable to apply CoS to L2TP session *session-id* because session-aware CoS is not enabled for interface *interface-name*

Description The class-of-service (CoS) process (cosd) did not apply CoS settings to the indicated Layer 2 Tunneling Protocol (L2TP) session on the indicated interface, because the interface is not configured to support session-aware CoS for L2TP. In terms of configuration, the 'per-session-scheduler' statement is not included at the [edit interfaces <interface-name> unit <logical-unit-number>] hierarchy level.

Type Error: An error occurred

Severity error

Action Include the 'per-session-scheduler' statement in the configuration for the interface.

COSD_L2TP_COS_NOT_SUPPORTED

System Log Message Unable to apply CoS to L2TP session *session-id* on interface *interface-name*: it does not support CoS

Description The class-of-service (CoS) process (cosd) did not apply CoS settings to the indicated Layer 2 Tunneling Protocol (L2TP) session on the indicated interface. The interface is configured to support session-aware CoS for L2TP, but is not on a Physical Interface Card (PIC) that supports that feature, such as an IQ2 PIC. In terms of configuration, the 'per-session-scheduler' statement is included at the [edit interfaces <interface-name> unit <logical-unit-number>] hierarchy level.

Type Error: An error occurred

Severity error

Action Determine whether the interface is on an PIC that supports session-aware CoS; if not, remove the 'per-session-scheduler' statement.

COSD_L2TP_SHAPING_NOT_CONFIGURED

System Log Message Unable to apply CoS to L2TP session *session-id* because session-aware shaping is not enabled for interface *interface-name*

Description The class-of-service (CoS) process (cosd) did not apply CoS settings to the indicated Layer 2 Tunneling Protocol (L2TP) session on the indicated interface, because session-aware traffic shaping for L2TP is not configured on the Physical Interface Card (PIC) that houses the interface. In terms of configuration, the 'session-shaping' statement is not included at the [edit chassis fpc <slot-number> pic <pic-number> traffic-manager mode] hierarchy level.

Type Error: An error occurred

Severity error

Action Include the 'session-shaping' statement in the configuration for the PIC.

COSD_LARGE_DELAY_BUFFER_INVALID

System Log Message Error for interface *interface-name error-message*

Description The class-of-service (CoS) process (cosd) did not apply the large delay buffer setting that is configured for the indicated interface.

Type Error: An error occurred

Severity error

Cause The interface is not housed on one of the Physical Interface Card (PIC) types that supports large delay buffer.

Action Remove the large delay buffer configuration from the interface.

COSD_MALLOC_FAILED

System Log Message malloc failed: *error-message*

Description The class-of-service (CoS) process (cosd) could not dynamically allocate memory, for the indicated reason.

Type Error: An error occurred

Severity error

Cause A software bug caused a memory leak, or the Routing Engine did not have sufficient memory.

Action Contact your technical support representative.

COSD_MULTILINK_CLASS_CONFLICT

System Log Message Fragmentation map *fragmentation-map* for wildcard *wildcard-interface-name* specified multilink class *class-name* for queue *queue-number* on interface *interface-name*, which exceeds configured limit of *limit*

Description The indicated fragmentation map is normally applied to interfaces that match the indicated wildcard, and specifies the indicated multilink class setting for queues on those interfaces. The class-of-service (CoS) process (cosd) did not apply the fragmentation map to the indicated interface, even though it matches the wildcard, because the setting in the map exceeds the indicated class limit, which is configured on the interface itself.

Type Error: An error occurred

Severity warning

Action Correct the configuration so that the multilink class setting in the fragmentation map does not exceed the class limit for the interface.

COSD_RATE_LIMIT_NOT_SUPPORTED

System Log Message Unable to apply scheduler map *scheduler-map* to interface *interface-name* because it does not support rate limiting

Description The class-of-service (CoS) process (cosd) did not apply the indicated scheduler map to the indicated interface, because a scheduler named in the scheduler map is configured for rate limiting. The interface is housed in a type of Physical Interface Card (PIC) that does not support rate limiting. In terms of configuration, the 'rate-limit' statement is included in the scheduler definition at the [edit class-of-service schedulers < scheduler-name > transmit-rate < rate > | percent < percentage >] hierarchy level. The scheduler is included in the scheduler map applied to the interface.

Type Error: An error occurred

Severity error

Action Remove the 'rate-limit' statement from the scheduler in the scheduler map applied to the interface.

COSD_REWRITE_RULE_LIMIT_EXCEEDED

System Log Message Number of rewrite rules applied to interface *interface-name* exceeds limit (*maximum-value*)

Description The class-of-service (CoS) process (cosd) determined that the number of rewrite rules applied to the indicated interface exceeds the indicated limit for the interface. In terms of configuration, too many rewrite rules are included at the [edit class-of-service interfaces < interface-name > unit < logical-unit-number > rewrite-rules] hierarchy level.

Type Error: An error occurred

Severity error

Action Remove rewrite rules from the configuration for the interface.

COSD_SCHEDULER_MAP_CONFLICT

System Log Message Forwarding classes "*first-forwarding-class*" and "*second-forwarding-class*" in scheduler map *scheduler-map* both map to queue *queue-number*

Description Both of the indicated forwarding classes, which are defined in the indicated scheduler map, map to the same indicated queue. The double mapping is invalid.

Type Error: An error occurred

Severity error

Action Map only one forwarding class to the queue.

COSD_STREAM_IFD_CREATE_FAILURE

System Log Message Unable to create special master interface device for *interface-name*

Description The class-of-service (CoS) process (cosd) could not create the indicated internal interface device, which it needs for application of a chassis scheduler map.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

COSD_TIMER_ERROR

System Log Message Unable to set retry timer for rtsock write operation: *error-message*

Description The class-of-service (CoS) process (cosd) used a routine from the rtsock library to write to the kernel, but the kernel did not accept the request. The cosd process could not set the retry timer for the request, for the indicated reason.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

COSD_TRICOLOR_NOT_SUPPORTED

System Log Message Unable to apply scheduler *scheduler-map* to interface *interface-name*, because it does not support tricolor marking

Description The class-of-service (CoS) process (cosd) did not apply the indicated scheduler map to the indicated interface, because a scheduler included in the map specifies a packet loss priority (PLP) that is supported only with tricolor marking (TCM). The interface does not support TCM, either because TCM is not enabled or the interface is on a router that does not support TCM. In terms of configuration, the value 'medium-high' or 'medium-low' is specified for the 'loss-priority' statement in a scheduler definition at the [edit class-of-service schedulers < scheduler-name > drop-profile-map] hierarchy level. The scheduler is included in the scheduler map applied to the interface, but the 'tri-color' statement is either not included at the [edit class-of-service] hierarchy level, or is not supported.

Type Error: An error occurred

Severity error

Action Change the value of the 'loss-priority' statement in the scheduler or include the 'tri-color' statement to enable TCM on the router.

COSD_TX_QUEUE_RATES_TOO_HIGH

System Log Message Unable to apply scheduler map *scheduler-map* to interface *interface-name*: sum of scheduler transmission rates exceeds interface shaping or transmission rate

Description The class-of-service (CoS) process (cosd) did not apply the indicated scheduler map to the indicated interface, because the sum of the queue transmission rates defined in the schedulers in the scheduler map exceeds the shaping or transmission rate for the interface. In terms of configuration, the 'transmit-rate' statement is specified for each scheduler at the [edit class-of-service schedulers < scheduler-name >] hierarchy level. The sum of the configured transmission rates exceeds the transmission or shaping rate of the interface.

Type Error: An error occurred

Severity error

Action Decrease the value of one or more 'transmit-rate' statements so that the sum is less than the interface transmission or shaping rate.

COSD_UNKNOWN_CLASSIFIER

System Log Message classifier type *classifier-type* is invalid

Description The class-of-service (CoS) process (cosd) did not recognize the indicated classifier type from the rtsock library.

Type Error: An error occurred

Severity warning

Cause An internal software failure occurred.

Action Contact your technical support representative.

COSD_UNKNOWN_REWRITE

System Log Message rtsock rewrite type *type* is invalid

Description The class-of-service (CoS) process (cosd) did not recognize the indicated rewrite type from the rtsock library.

Type Error: An error occurred

Severity warning

Cause An internal software failure occurred.

Action Contact your technical support representative.

Chapter 18

DCD System Log Messages

This chapter describes messages with the DCD prefix. They are generated by the interface process (dcd), which controls the physical interface devices and logical interfaces in the routing platform.

DCD_MALLOC_FAILED_INIT

System Log Message Memory allocation failed during initialization for configuration load

Description The interface process (dcd) could not dynamically allocate memory in preparation for loading a configuration.

Type Error: An error occurred

Severity error

Cause A software bug caused a memory leak, or the routing platform had insufficient memory.

Action Contact your technical support representative.

DCD_PARSE_EMERGENCY

System Log Message dcd_config: errors while parsing configuration file

Description The interface process (dcd) encountered an unhandled internal state while parsing the configuration database.

Type Error: An error occurred

Severity error

Cause There might be a bug in the dcd process' parser.

Action Contact your technical support representative.

DCD_PARSE_ERROR_CLOCK

System Log Message PIC housing interface *interface-name* does not support clocking as configured

Description The 'clocking' statement is included at the [edit interfaces] hierarchy level for the indicated interface, but is not supported by the 10-Gigabit Ethernet IQ2 Physical Interface Card (PIC).

Type Error: An error occurred

Severity warning

Action Remove the 'clocking' statement from the configuration for the interface.

DCD_PARSE_ERROR_HIER_SCHEDULER

System Log Message *interface-name*: PIC or encapsulation type does not support 'hierarchical-scheduler' statement

Description The 'hierarchical-scheduler' statement is included at the [edit interfaces] hierarchy level for the indicated interface, but is not supported either by the PIC or the configured type of encapsulation.

Type Error: An error occurred

Severity warning

Action Remove the 'hierarchical-scheduler' statement from the configuration for the interface.

DCD_PARSE_ERROR_IFLSET

System Log Message Interface *interface-name* does not support 'interface-set' statement

Description The 'interface-set' statement is included at the [edit interfaces] hierarchy level for the indicated interface, but is not supported by the interface.

Type Error: An error occurred

Severity warning

Action Remove the 'interface-set' statement from the configuration for the interface.

DCD_PARSE_ERROR_SCHEDULER

System Log Message *interface-name*: PIC or encapsulation type does not support 'per-unit-scheduler' or 'shared-scheduler' statement

Description The 'per-unit-scheduler' or 'shared-scheduler' statement is included at the [edit interfaces] hierarchy level for the indicated interface, but is not supported either by the PIC or the configured type of encapsulation.

Type Error: An error occurred

Severity warning

Action Remove the 'per-unit-scheduler' or 'shared-scheduler' statement from the configuration for the interface.

DCD_PARSE_ERROR_SCHEDULER_LIMIT

System Log Message *interface-name*: exceeds the allowed limit (*maximum-value*) of 'per-unit-scheduler' interface statement for PIC = *pic-slot* on FPC = *fpc-slot*

Description The 'per-unit-scheduler' statement is enabled on more interfaces than what this PIC would suppport.

Type Error: An error occurred

Severity warning

Action Remove the 'per-unit-scheduler' statement from the configuration for the interface.

DCD_PARSE_ERROR_VLAN_TAGGING

System Log Message *interface-name*: PIC type does not support flexible-vlan-tagging statement

Description The 'flexible-vlan-tagging' statement is included at the [edit interfaces] hierarchy level for the indicated interface, but is not supported by the Physical Interface Card (PIC) that houses the interface.

Type Error: An error occurred

Severity warning

Action Remove the 'flexible-vlan-tagging' statement from the configuration for the interface.

DCD_PARSE_MINI_EMERGENCY

System Log Message dcd_mini_config: errors while parsing configuration overlay

Description The interface process (dcd) encountered an unhandled internal state during interface parsing.

Type Error: An error occurred

Severity error

Cause There might be a bug in the dcd process' parser.

Action Contact your technical support representative.

DCD_PARSE_STATE_EMERGENCY

System Log Message An unhandled state was encountered during interface parsing

Description The interface process (dcd) encountered an unhandled internal state during interface parsing.

Type Error: An error occurred

Severity emergency

Cause There might be a bug in the dcd process' parser.

Action Contact your technical support representative.

Chapter 19

DFCD System Log Messages

This chapter describes messages with the DFCD prefix. They are generated by the dynamic flow control process (dfcd), which monitors packet flows using dynamically alterable filtering criteria.

DFCD_FTAP_PIC_UNSUPPORTED

System Log Message PIC housing interface *interface-name* does not support flow-tap service

Description The Physical Interface Card (PIC) that houses the indicated interface does not support flow-tap service.

Type Error: An error occurred

Severity error

DFCD_GENCFG_MALLOC_FAILED

System Log Message GENCFG mem alloc failed !!!

Description The dynamic flow capture process (dfcd) could not allocate memory for gencfg message.

Type Error: An error occurred

Severity error

DFCD_GENCFG_WRITE_FAILED

System Log Message GENCFG write failed for Reason: *error-message* (*error-code*)

Description The dynamic flow capture process (dfcd) could not send gencfg message, for the indicated reason.

Type Error: An error occurred

Severity error

DFCD_LINH_MALLOC_FAILED

System Log Message GENCFG mem alloc failed !!!

Description The dynamic flow capture process (dfcd) could not allocate memory for linh message.

Type Error: An error occurred

Severity error

DFCD_LI_NEXT_HOP_ADD_FAILED

System Log Message Unable to add li next hop for subscriber interface: *error-message* (*error-code*)

Description The dynamic flow capture process (dfcd) could not add a subscriber li next hop, for the indicated reason.

Type Error: An error occurred

Severity error

DFCD_NEXT_HOP_ADD_FAILED

System Log Message Unable to add service next hop: *error-message* (*error-code*)

Description The dynamic flow capture process (dfcd) could not add a service next hop, for the indicated reason.

Type Error: An error occurred

Severity error

DFCD_NEXT_HOP_DELETE_FAILED

System Log Message Unable to delete service next hop: *error-message* (*error-code*)

Description The dynamic flow capture process (dfcd) could not delete a service next hop, for the indicated reason.

Type Error: An error occurred

Severity error

DFCD_SAMPLE_CLASS_ADD_FAILED

System Log Message Unable to add sample class: *error-message* (*error-code*)

Description The dynamic flow capture process (dfcd) could not add a sample class, for the indicated reason.

Type Error: An error occurred

Severity error

DFCD_SAMPLE_CLASS_DELETE_FAILED

System Log Message Unable to delete sample class: *error-message* (*error-code*)

Description The dynamic flow capture process (dfcd) could not delete a sample class, for the indicated reason.

Type Error: An error occurred

Severity error

Chapter 20

DFWD System Log Messages

This chapter describes messages with the DFWD prefix. They are generated by the firewall process (dfwd), which manages compilation and downloading of JUNOS firewall filters.

DFWD_MALLOC_FAILED_INIT

System Log Message Memory allocation failed during initialization for configuration load

Description The firewall process (dfwd) could not dynamically allocate memory in preparation for loading a configuration.

Type Error: An error occurred

Severity error

Cause A software bug caused a memory leak, or the routing platform had insufficient memory.

Action Contact your technical support representative.

DFWD_PARSE_FILTER_EMERGENCY

System Log Message dfwd encountered errors while parsing filter index file

Description The firewall process (dfwd) encountered an unhandled internal state while parsing a filter index file.

Type Error: An error occurred

Severity error

Cause There might be a bug in the parser.

Action Contact your technical support representative.

DFWD_PARSE_STATE_EMERGENCY

System Log Message dfwd encountered unhandled state while parsing interface

Description The firewall process (dfwd) encountered an unhandled internal state while parsing an interface.

Type Error: An error occurred

Severity emergency

Cause There might be a bug in the parser.

Action Contact your technical support representative.

Chapter 21

DHCPD System Log Messages

This chapter describes messages with the DHCPD prefix. They are generated by the Dynamic Host Configuration Protocol (DHCP) server process (dhcpd) for J-series Services Routers, which automatically allocates network IP addresses and delivers configuration settings to client hosts in a Transmission Control Protocol (TCP)/IP network.

DHCPD_BIND_FAILURE

System Log Message bind() to port *port* failed: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) received the indicated error when it tried to bind a socket to the indicated local port.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

DHCPD_DEGRADED_MODE

System Log Message Running in degraded mode because of *reason*: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) began running in degraded mode because the indicated unrecoverable error occurred.

Type Error: An error occurred

Severity error

Cause There might be a problem with the lease cache directory used to store persistent lease information.

Action Contact your technical support representative.

DHCPD_MEMORY_ALLOCATION_FAILURE

System Log Message Unable to allocate memory for *object-name*: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not allocate memory from the heap for the indicated object.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

DHCPD_OVERLAY_CONFIG_FAILURE

System Log Message Unable to open overlay configuration: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not open an overlay configuration file for parsing.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

DHCPD_OVERLAY_PARSE_FAILURE

System Log Message Unable to parse overlay configuration because of *count* syntax errors

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not parse its overlay configuration because the configuration contained the indicated number of syntax errors.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

DHCPD_RECVMSG_FAILURE

System Log Message Exiting due to too many recvmsg() failures

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not receive data from the network, which it needs to do during normal operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

DHCPD_RTSOCK_FAILURE

System Log Message Error with rtsock: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) experienced the indicated error with a routing socket.

Type Error: An error occurred

Severity info

Cause An internal software failure occurred.

Action Contact your technical support representative.

DHCPD_SENDMSG_FAILURE

System Log Message sendmsg() from *source-address* to port *destination-port* at *destination-address* via interface *interface-name* and routing instance *routing-instance* failed: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not send data from the indicated source (address, interface, and routing instance) to the indicated destination (port and address), which it needs to do during normal operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

DHCPD_SENDMSG_NOINT_FAILURE

System Log Message sendmsg() from *source-address* to port *destination-port* at *destination-address* via routing instance *routing-instance* failed: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not send data from the indicated source (address and routing instance) to the indicated destination (port and address), which it needs to do during normal operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

DHCPD_SETSOCKOPT_FAILURE

System Log Message setsockopt(*socket-option*) failed: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not set the indicated socket option.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

DHCPD_SOCKET_FAILURE

System Log Message socket(*arguments*) failed: *error-message*

Description The Dynamic Host Configuration Protocol server process (dhcpd) could not create a socket.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

Chapter 22

ESWD System Log Messages

This chapter describes messages with the ESW prefix. They are generated by the Ethernet Switching process (eswd), which maintains the timeout (lease time) value for each IP-address–MAC-address binding in its database.

ESWD_BPDU_BLOCK_ERROR_DISABLED

System Log Message *interface-name*: bpdu-block disabled port

Description This condition occurs when bpdu-block error condition is detected

Type Error: An error occurred

Severity alert

ESWD_BPDU_BLOCK_ERROR_ENABLED

System Log Message *interface-name*: bpdu-block enabled port

Description This condition occurs when bpdu-block error condition is cleared

Type Error: An error occurred

Severity alert

ESWD_INVALID_MAC_ADDRESS

System Log Message Invalid MAC address *mac-addresse* received on *interface-name*

Description Received a MAC address that is not in the configured valid MAC addresses for this interface.

Type Error: An error occurred

Severity alert

Cause MAC address recieved is not configured as a valid MAC address for this interface.

ESWD_MAC_LIMIT_BLOCK

System Log Message MAC limit (*limit*) exceeded at *interface-name*: shutting down the interface

Description Interface was blocked because the number of MAC addresses learned on an interface has exceeded the user configured limit.

Type Error: An error occurred

Severity alert

Cause More learning requests were received by the system than the user configured.

ESWD_MAC_LIMIT_DROP

System Log Message MAC limit (*limit*) exceeded at *interface-name*: dropping the packet

Description Learning request was dropped because the number of MAC addresses learned on an interface has reached the user configured limit.

Type Error: An error occurred

Severity alert

Cause More learning requests were received by the system than the user configured.

ESWD_MAC_LIMIT_EXCEEDED

System Log Message MAC limit (*limit*) exceeded at *interface-name*

Description Number of MAC addresses learned on an interface has exceeded the user configured limit.

Type Error: An error occurred

Severity alert

Cause More learning requests were received by the system than the user configured.

ESWD_MAC_MOVE_LIMIT_BLOCK

System Log Message MAC move limit (*limit*) exceeded at *vlan-name*; shutting down interface *interface-name*

Description Data traffic on interface was halted because the number of times that a MAC addresses moved to a different interface exceeded the user-configured limit.

Type Error: An error occurred

Severity alert

Cause A MAC address moved to a different interface more times per second than the user configured.

ESWD_MAC_MOVE_LIMIT_DROP

System Log Message MAC move limit (*limit*) exceeded at *vlan-name*; dropping the packet on interface *interface-name*

Description Learning request was dropped because the number of times a MAC address moved to a different interface exceeded the user-configured limit.

Type Error: An error occurred

Severity alert

Cause A MAC address moved to a different interface more times per second than the user configured.

ESWD_MAC_MOVE_LIMIT_EXCEEDED

System Log Message MAC move limit (*limit*) exceeded at *vlan-name*

Description The number of times that a MAC address moved to a different interface within a VLAN exceeded the user-configured limit.

Type Error: An error occurred

Severity alert

Cause A MAC address moved to a different interface more times per second than the user configured.

ESWD_MIRROR_ERROR

System Log Message Mirror version on other Routing Engine is incompatible: *error-message*

Description The indicated error occurred when the layer2 control protocol process (l2cpd) tried to establish the nonstop routing mirror connection between the master and standby Routing Engines.

Type Error: An error occurred

Severity warning

Cause The master and standby Routing Engines are running incompatable versions of the JUNOS software.

Action Update the JUNOS software on the master Routing Engine, standby Routing Engine, or both, so that they are running compatible versions.

ESWD_MIRROR_VERSION_MISMATCH

System Log Message Mirror versions on Routing Engines are incompatible: master*master-is-local* has version *master-version*, standby*standby-is-local* has version *standby-version*

Description While trying to establish the nonstop routing mirror connection between the master and standby Routing Engines, the layer2 control protocol process (l2cpd) determined that the version of the nonstop routing mirror software on the Routing Engines did not match.

Type Error: An error occurred

Severity warning

Cause The master and standby Routing Engines are running incompatable versions of the JUNOS software.

Action Update the JUNOS software on the master Routing Engine, standby Routing Engine, or both, so that they are running compatible versions.

ESWD_MODULE_SHUTDOWN_FAILURE

System Log Message ESWD: *error-message* Module shutdown failed

Description While deleting the instance of logical-switch, RST/MST Module shutdown failed

Type Error: An error occurred

Severity error

ESWD_PPM_READ_ERROR

System Log Message Read error on pipe from ppmd: *reason* (*error-message*)

Description The ethernet bridging process (eswd) could not read a message available on the read pipe from the periodic packet management process (ppmd).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

ESWD_PPM_WRITE_ERROR

System Log Message *function-name*: write error on pipe to ppmd (*error-message*)

Description The ethernet bridging process (eswd) could not write a message on the pipe to the periodic packet management process (ppmd).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

ESWD_SYSTEM_CALL_FAILED

System Log Message *reason*: *error-message*

Description A system call made by enterprise switching process (eswd) failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request.

Chapter 23

EVENTD System Log Messages

This chapter describes messages with the EVENTD prefix. They are generated by the event policy process (eventd), which performs configured actions in response to events on a routing platform that trigger system log messages.

EVENTD_ACK_FAILED

System Log Message Unable to send acknowledgment: *error-message*

Description JUNOS processes can request that the event processing process (eventd) notify them when a specific event occurs. The eventd process could not send an acknowledgment for a registration request, for the indicated reason.

Type Error: An error occurred

Severity error

EVENTD_COMMAND_SUBSTITUTE_ERROR

System Log Message Variable substitution failed for command '*command*'

Description The event processing process (eventd) can be configured to execute a JUNOS command-line interface (CLI) command when a specified event occurs. The command can include one or more variables (such as an interface name), which the eventd process replaces with actual values related to the event when it issues the command. Variable substitution failed for the indicated command.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

EVENTD_EVENT_SEND_FAILED

System Log Message Unable to send event notification: *error-message*

Description JUNOS processes can request that the event processing process (eventd) notify them when a specific event occurs. The eventd process could not send an event notification for the indicated reason.

Type Error: An error occurred

Severity error

EVENTD_FORK_ERR

System Log Message Unable to fork: *error-message*

Description The event processing process (eventd) could not create a child process for executing policies.

Type Error: An error occurred

Severity error

EVENTD_PIPE_CREATION_FAILED

System Log Message Unable to create pipe: *error-message*

Description The event processing process (eventd) could not create a pipe for interprocess communication.

Type Error: An error occurred

Severity error

EVENTD_POLICY_ACTION_FAILED

System Log Message Unable to execute '*action*' action in policy *policy-name*

Description The event processing process (eventd) could not perform the indicated action, which is specified by the indicated policy.

Type Error: An error occurred

Severity error

EVENTD_POLICY_LIMIT_EXCEEDED

System Log Message Unable to execute policy '*policy-name*' because current number of policies (*count*) exceeds system limit (*limit*)

Description The event processing process (eventd) could not execute the indicated policy, because the indicated number of currently executing policies exceeded the indicated maximum defined by the system.

Type Event: This message reports an event, not an error

Severity warning

EVENTD_POLICY_UPLOAD_FAILED

System Log Message Unable to upload file '*filename*' to destination '*destination-name*' for policy '*policy-name*'

Description The event processing process (eventd) could not upload the indicated file to the indicated destination.

Type Error: An error occurred

Severity error

EVENTD_POPEN_FAIL

System Log Message Error *error-code* in invoking command '*command*'

Description A call to the popen() function failed when the event processing process (eventd) invoked the indicated command.

Type Error: An error occurred

Severity error

EVENTD_READ_ERROR

System Log Message recvmsg() failed: *error-message*

Description The event processing process (eventd) could not read an event sent to it, for the indicated reason.

Type Error: An error occurred

Severity error

EVENTD_REGEXP_INVALID

System Log Message Invalid regular expression '*regular-expression*' provided for attribute value

Description The event processing process (eventd) received a request that included the indicated regular expression as the value for an attribute. The regular expression is not valid.

Type Error: An error occurred

Severity error

EVENTD_REG_VERSION_MISMATCH

System Log Message Registration version *expected-value* did not match expected version (*received-value*)

Description The event processing process (eventd) received a registration request with the indicated version indicator, which does not match the indicated version expected by the eventd process.

Type Error: An error occurred

Severity error

EVENTD_ROTATE_COMMAND_FAILED

System Log Message Command '*command*' failed during rotation of file '*filename*': *error-message*

Description The event processing process (eventd) invoked the indicated command while attempting to rotate the indicated file. The command failed.

Type Error: An error occurred

Severity error

EVENTD_ROTATE_FORK_EXCEEDED

System Log Message Unable to fork: too many child processes

Description The event processing process (eventd) could not create a child process for rotating files because adding another child would have made the number of children exceed the limit.

Type Error: An error occurred

Severity error

EVENTD_ROTATE_FORK_FAILED

System Log Message Unable to fork: *error-message*

Description The event processing process (eventd) could not create a child process for rotating files, for the indicated reason.

Type Error: An error occurred

Severity error

EVENTD_SET_PROCESS_PRIV_FAILED

System Log Message Unable to set process privilege level to that of user '*username*': *error-message*

Description In preparation for executing an action defined in a policy, the event processing process (eventd) tried to change its privilege level to that of the indicated JUNOS user. The attempt failed. It made the attempt because the user-name statement is included at one of several possible levels under the [edit event-options policy <policy-name> then] hierarchy level.

Type Error: An error occurred

Severity error

EVENTD_SET_TIMER_FAILED

System Log Message evSetTimer failed: *error-message*

Description The event processing process (eventd) starts a timer whenever an internal event needs to be generated. It could not activate the timer for the indicated reason.

Type Error: An error occurred

Severity error

EVENTD_SYSLOG_FWD_FAILED

System Log Message Unable to forward syslog message to PSD (*psd-id*), errorno: *error-code*

Description The event processing process (eventd) encountered a system error when forwarding a syslog message to indicated protected system domain (PSD).

Type Error: An error occurred

Severity error

EVENTD_TRANSFER_COMMAND_FAILED

System Log Message Command '*error-code*' failed during transfer of file '*command*': *filename*

Description The event processing process (eventd) invoked the indicated command while attempting to transfer the indicated file. The command failed.

Type Error: An error occurred

Severity error

EVENTD_TRANSFER_FORK_EXCEEDED

System Log Message Unable to fork: too many child processes

Description The event processing process (eventd) could not create a child process for transferring files, because adding another child would have made the number of children exceed the limit.

Type Error: An error occurred

Severity error

EVENTD_TRANSFER_FORK_FAILED

System Log Message Unable to fork: *error-message*

Description The event processing process (eventd) could not create a child process for transferring files, for the indicated reason.

Type Error: An error occurred

Severity error

EVENTD_VERSION_MISMATCH

System Log Message Event version *expected-value* did not match expected version (*received-value*)

Description The event processing process (eventd) received an event with the indicated version indicator, which does not match the indicated version expected by the eventd process.

Type Error: An error occurred

Severity error

EVENTD_XML_FILENAME_INVALID

System Log Message XML syntax of output filename was invalid

Description An event script created an output file and wrote the filename to standard output (stdout) with Extensible Markup Language (XML) tagging like the following: < event-script-output-filename > output-file.tgz < /event-script-output-filename > . The event processing process read the output filename and determined that its XML syntax was invalid.

Type Error: An error occurred

Severity error

Chapter 24

FLOW System Log Messages

This chapter describes messages with the FLOW prefix. They are generated by the process that handles flows on routers running the JUNOS software with enhanced services.

FLOW_HIGH_WATERMARK_TRIGGERED

System Log Message Number of sessions *current-flows* exceeded the high watermark *limit*. Early aging triggered.

Description Early aging of sessions is triggered when the number of concurrent session entries in the session table exceeds the configured high watermark. When the number of concurrent sessions drops below the configured low watermark, the router stops aggressively aging out sessions. This message notifies you that the session high watermark has been exceeded and aggressive aging of sessions has begun.

Type Event: This message reports an event, not an error

Severity info

FLOW_IP_ACTION

System Log Message Flow IP action detected attack attempt: *source-address*/*source-port* -- > *destination-address*/*destination-port* from interface *interface-nameaction*.

Description Flow IP action detected attack attempt.

Type Event: This message reports an event, not an error

Severity info

FLOW_LOW_WATERMARK_TRIGGERED

System Log Message Number of sessions *current-flows* dropped below the low watermark *limit*. Early aging stopped.

Description Early aging of sessions is triggered when the number of concurrent session entries in the session table exceeds the configured high watermark. When the number of concurrent sessions drops below the configured low watermark, the router stops aggressively aging out sessions. This message notifies you that the number of concurrent sessions has dropped below the configured low watermark, and that aggressive aging of sessions has stopped.

Type Event: This message reports an event, not an error

Severity info

FLOW_SESSION_CLOSE

System Log Message session closed *reason*:
source-address/*source-port*- > *destination-address*/*destination-port*,*protocol-id*:
policy-name, *inbound-packets*, *inbound-bytes*,*outbound-bytes elapsed-time*

Description A security session was closed.

Type Event: This message reports an event, not an error

Severity info

FLOW_SESSION_CREATE

System Log Message session created
source-address/*source-port*- > *destination-address*/*destination-port*,*protocol-id*:
policy-name

Description A security session was created.

Type Event: This message reports an event, not an error

Severity info

FLOW_SESSION_DENY

System Log Message session denied
source-address/*source-port*- > *destination-address*/*destination-port*,*protocol-id*(*icmp-type*):
policy-name

Description A security session was not permitted by policy.

Type Event: This message reports an event, not an error

Severity info

Chapter 25

FPCLOGIN System Log Messages

This chapter describes messages with the FPCLOGIN prefix. They are generated by the Flexible PIC Concentrator (FPC) login process (pimlogin), which provides direct login access to Physical Interface Modules (PIMs).

FPCLOGIN_ADDRESS_GET_FAILED

System Log Message Unable to determine IP address of TGM in slot *slot*

Description A user tried to log in to the Physical Interface Module (PIM) in the indicated slot on a Flexible PIC Concentrator (FPC). In response, the FPC login process (pimlogin) tried to determine the PIM's IP address. It could not do so, and the login attempt failed.

Type Error: An error occurred

Severity error

FPCLOGIN_IPC_RECEIVE_FAILED

System Log Message Unable to receive IPC message from *process-name*

Description The Flexible PIC Concentrator (FPC) login process (pimlogin) could not process an interprocess communication (IPC) message from the indicated other process. The 'wxd' process is the WX Physical Interface Module process.

Type Error: An error occurred

Severity error

FPCLOGIN_IPC_SEND_FAILED

System Log Message Unable to send IPC message to *process-name*

Description The Flexible PIC Concentrator (FPC) login process (pimlogin) could not send an interprocess communication (IPC) message to the indicated other process. The 'wxd' process is the WX Physical Interface Module process (wxd).

Type Error: An error occurred

Severity error

FPCLOGIN_LOGIN_FAILED

System Log Message fpclogin failed: *error-message*

Description A user tried to log in to a Physical Interface Module (PIM). The attempt failed for the indicated reason.

Type Error: An error occurred

Severity error

FPCLOGIN_MESSAGE_INVALID

System Log Message Message from *process-name error-message*

Description The message that the Flexible PIC Concentrator (FPC) login process (pimlogin) received from the indicated other process was invalid in the indicated way. The 'wxd' process is the WX Physical Interface Module process (wxd).

Type Error: An error occurred

Severity error

FPCLOGIN_SOCKET_OPERATION_FAILED

System Log Message Unable to complete '*error-message*' operation

Description The Flexible PIC Concentrator (FPC) login process (pimlogin) could not perform the indicated operation on a routing socket.

Type Error: An error occurred

Severity error

Chapter 26

FSAD System Log Messages

This chapter describes messages with the FSAD prefix. They are generated by the File System Access process (fsad), which provides Trivial FTP (TFTP) support for file transfer between services Physical Interface Cards (PICs) and other routing platform components.

FSAD_CONFIG_ERROR

System Log Message Reason: *reason*

Description The configuration file for the File System Access process (fsad) might contain an error.

Type Error: An error occurred

Severity error

FSAD_CONNTIMEDOUT

System Log Message Connection timed out to the client (*connection-type*, *ip-address*) having request type *port*

Description The File System Access process (fsad) flushed all state information about the timed-out connection.

Type Event: This message reports an event, not an error

Severity error

FSAD_DIR_CREATE

System Log Message Failed to create directory *directory-name*: *error-message*

Description The File System Access process (fsad) could not create the indicated directory.

Type Error: An error occurred

Severity error

FSAD_DIR_STAT

System Log Message *function-name*: stat() failed for pathname *pathname*: *reason*

Description The File System Access process (fsad) received a request for a nonexistent file or directory.

Type Error: An error occurred

Severity error

Cause The path does not exist.

Action Make sure the path specified in the request is valid.

FSAD_FAILED

System Log Message In *enclosing-function-name*: *function-name*() returned: *reason*

Description An internal error occurred inside a function in the File System Access process (fsad).

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

FSAD_FILE_FAILED

System Log Message *enclosing-function-name*: *function-name* failed for file '*filename*' with error message *reason*

Description An internal error occurred while the File System Access process (fsad) was performing a file operation.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

FSAD_FILE_REMOVE

System Log Message Unable to remove file '*filename*': *reason*

Description The File System Access process (fsad) could not remove the indicated file for the indicated reason.

Type Error: An error occurred

Severity error

Cause The file to be removed does not exist or its permissions do not allow the operation.

Action Make sure that the file exists and that its permissions allow it to be deleted.

FSAD_FILE_RENAME

System Log Message Unable to rename file '*source-filename*' to '*destination-filename*': *reason*

Description The File System Access process (fsad) could not rename the indicated file for the indicated reason.

Type Error: An error occurred

Severity error

Cause Either the source file does not exist, or one or both of the source and destination pathnames are incorrect.

Action Make sure the source and destination paths exist and that the rename operation is allowed.

FSAD_FILE_STAT

System Log Message *function-name*: stat() failed for file pathname *pathname*: *reason*

Description The File System Access process (fsad) received a request for a nonexistent file.

Type Error: An error occurred

Severity error

Cause The file path does not exist.

Action Make sure the path specified in the request is valid.

FSAD_FILE_SYNC

System Log Message Unable to sync file '*filename*': *reason*

Description When closing a file, the File System Access process (fsad) executes the sync() system call to ensure that any changes to the file are committed to disk. This operation failed for the indicated file.

Type Error: An error occurred

Severity error

FSAD_FLOWC_IPC_PAYLOAD_SIZE

System Log Message Received flowc IPC message with incorrect length: message type *message-type*, subtype *message-subtype*, opcode *operation-code*, length *length* (expected length *expected-value*)

Description The File System Access process (fsad) received a flow collector IPC message in which the payload length was incorrect.

Type Error: An error occurred

Severity error

FSAD_FLOWC_IPC_SUBTYPE

System Log Message Received flowc IPC message with incorrect subtype: message type *message-type*, subtype *message-subtype*, opcode *operation-code*, length *length*

Description The File System Access process (fsad) received a flow collector IPC message in which the subtype field was incorrect.

Type Error: An error occurred

Severity error

FSAD_FLOWC_IPC_TYPE

System Log Message Received flowc IPC message with incorrect type: message type *message-type*, subtype *message-subtype*, opcode *operation-code*, length *length*

Description The File System Access process (fsad) received a flow collector IPC message in which the type field was incorrect.

Type Error: An error occurred

Severity error

FSAD_FLOWC_IPC_VERSION

System Log Message Received flowc IPC message with incorrect version *received-value* (expected version *expected-value*)

Description The File System Access process (fsad) received a flow collector IPC message in which the version field was incorrect.

Type Error: An error occurred

Severity error

FSAD_FLOWC_SERVICE_INACTIVE

System Log Message *reason*

Description The File System Access process (fsad) received a request for the Flow Collector Transfer Log Archive service, which is not currently active.

Type Error: An error occurred

Severity error

FSAD_FREE_SPACE_LOG

System Log Message Unable to move temporary file *temporary-filename* (size *file-size* KB) to log file *log-filename* because free disk space (*count* KB) is insufficient

Description The File System Access process (fsad) could not move the CDR temporary file of the indicated size to the log file, because it is larger than the amount of free disk space.

Type Error: An error occurred

Severity error

FSAD_FREE_SPACE_TMP

System Log Message Unable to write CDR batch output to file *temporary-filename* because free disk space (*count* KB) is insufficient

Description The File System Access process (fsad) could not write CDR batch output to the indicated temporary file, because the amount of free disk space was insufficient.

Type Error: An error occurred

Severity error

FSAD_FS_STAT

System Log Message statfs() failed for pathname *pathname*: *reason*

Description The File System Access process (fsad) encountered an error in getting filesystem statistics.

Type Error: An error occurred

Severity error

FSAD_GEN_IPC_PAYLOAD_SIZE

System Log Message Received IPC message with incorrect length: message type *message-type*, subtype *message-subtype*, opcode *operation-code*, length *length* (expected length *expected-value*)

Description The File System Access process (fsad) received an IPC message in which the payload length was incorrect.

Type Error: An error occurred

Severity error

FSAD_GEN_IPC_SUBTYPE

System Log Message Received IPC message with incorrect subtype: message type *message-type*, subtype *message-subtype*, opcode *operation-code*, length *length*

Description The File System Access process (fsad) received an IPC message in which the subtype field was incorrect.

Type Error: An error occurred

Severity error

FSAD_GEN_IPC_TYPE

System Log Message Received IPC message with incorrect type: message type *message-type*, subtype *message-subtype*, opcode *operation-code*, length *length*

Description The File System Access process (fsad) received an IPC message in which the type field was incorrect.

Type Error: An error occurred

Severity error

FSAD_GEN_IPC_VERSION

System Log Message Received generic IPC message with incorrect version *received-value* (expected version *expected-value*)

Description The File System Access process (fsad) received an IPC message in which the version field was incorrect.

Type Error: An error occurred

Severity error

FSAD_GEN_SERVICE_INACTIVE

System Log Message Received IPC message for inactive service *service-name*

Description The File System Access process (fsad) received an IPC message for a service that is currently not active.

Type Error: An error occurred

Severity error

FSAD_GEN_SERVICE_INIT_FAILED

System Log Message Failed to initialize service *service-name*

Description The File System Access process (fsad) could not initialize the indicated service.

Type Error: An error occurred

Severity error

FSAD_MAXCONN

System Log Message Upper limit reached in fsad for handling connections

Description The File System Access process (fsad) stopped accepting new connections because it reached an internal limit for handling connections.

Type Event: This message reports an event, not an error

Severity error

FSAD_MEMORYALLOC_FAILED

System Log Message *allocation-function-name* failed in the function *function-name* (*line-number*)

Description The File System Access process (fsad) could not allocate memory. The system might be running low on memory.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

FSAD_NOT_ROOT

System Log Message Must be run as root

Description The user who attempted to start the File System Access process (fsad) was not the root user.

Type Error: An error occurred

Severity error

FSAD_PARENT_DIRECTORY

System Log Message *directory-name*: invalid directory: *message*

Description The parent directory specified in the request for a file was not valid.

Type Error: An error occurred

Severity error

Action Make sure the path specified in the request is valid.

FSAD_PATH_IS_DIRECTORY

System Log Message File path cannot be a directory (*pathname*)

Description The File System Access process (fsad) received a request on a directory instead of a regular file.

Type Error: An error occurred

Severity error

Cause The file path points to a directory.

Action Make sure the path points to a regular file.

FSAD_PATH_IS_NOT_DIRECTORY

System Log Message invalid path '*pathname*' : not a directory : *action*

Description The File System Access process (fsad) received a request for a pathname that was not a directory.

Type Error: An error occurred

Severity error

FSAD_PATH_IS_SPECIAL

System Log Message Not a regular file (*pathname*)

Description The File System Access process (fsad) received a request for a pathname that points to a nonregular file.

Type Error: An error occurred

Severity error

Action Make sure the path points to a regular file.

FSAD_RECVERROR

System Log Message fsad received error *message* from client having request type *connection-type* at (*ip-address*, *port*)

Description The File System Access process (fsad) received a packet with the indicated error message from the other end of a connection.

Type Error: An error occurred

Severity error

FSAD_RENAME

System Log Message *function-name*: failed to rename temporary file *filename* to *new-filename*: *reason*

Description The File System Access process (fsad) could not rename the indicated temporary file for the indicated reason.

Type Error: An error occurred

Severity error

FSAD_TERMINATED_CONNECTION

System Log Message Open file '*filename*' closed due to process shutdown

Description The File System Access process (fsad) terminated a connection, stored the connection's (unwritten) data to disk, and purged it from its data structures.

Type Event: This message reports an event, not an error

Severity notice

FSAD_TRACEOPEN_FAILED

System Log Message Open operation on trace file '*pathname*' returned error *error-message*

Description The File System Access process (fsad) failed to open the indicated trace file.

Type Error: An error occurred

Severity error

FSAD_USAGE

System Log Message Incorrect usage, *message*

Description The File System Access process (fsad) displayed its usage statement.

Type Event: This message reports an event, not an error

Severity error

Cause The fsad process was invoked with incorrect command-line arguments.

Action Check the usage and invoke the fsad process with the correct command-line arguments.

Chapter 27

FUD System Log Messages

This chapter describes messages with the FUD prefix. They are generated by the UDP forwarding process (fud), which forwards UDP (User Datagram Protocol) packets from a network to a server for services that run over UDP.

FUD_ARGUMENT_FAILURE

System Log Message Unknown option "*option*"

Description One or more options provided on the 'fud' command line were invalid. The UDP forwarding process (fud) initialized but ignored the invalid options.

Type Error: An error occurred

Severity error

Action Reissue the 'fud' command with the correct options.

FUD_BAD_SERVER_ADDR_FAILURE

System Log Message Destination address of *destination-address* is invalid

Description One or more server addresses configured for the UDP forwarding process (fud) were invalid.

Type Error: An error occurred

Severity error

Action Reconfigure the fud process with valid server addresses.

FUD_BIND_FAILURE

System Log Message bind(port *port*) failed: *error-message*

Description The UDP forwarding process (fud) received the indicated error when it tried to bind a socket to a local address.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_DAEMON_FAILURE

System Log Message Unable to run in the background as daemon: *error-message*

Description The UDP forwarding process (fud) could not create a version of itself to run in the background as a daemon.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_MEMORY_ALLOCATION_FAILURE

System Log Message Unable to allocate *count* bytes of memory: *error-message*

Description The UDP forwarding process (fud) could not allocate the indicated amount of memory from the heap.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_PERMISSION_FAILURE

System Log Message *program-name* must be run as root

Description The user who attempted to start the UDP forwarding process (fud) was not the root user, so the process did not start.

Type Error: An error occurred

Severity error

Action Become the root user before issuing the 'fud' command.

FUD_PIDLOCK_FAILURE

System Log Message Unable to lock PID file; another *program-name* was running

Description The UDP Forwarding process (fud) attempted to lock the file that records its process ID (PID), which serves to prevent multiple instances of the fud process from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

Cause Another instance of the fud process is running.

Action Check whether another fud process is running, and stop it if appropriate.

FUD_PIDUPDATE_FAILURE

System Log Message Unable to update PID file for *program-name*

Description The UDP Forwarding process (fud) attempted to update the file that records its process ID (PID), which serves to prevent multiple instances of the fud process from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

Cause Another instance of the fud process is running.

Action Check whether another fud process is running, and stop it if appropriate.

FUD_RECVMSG_FAILURE

System Log Message Exiting because of repeated recvmsg() failures

Description The UDP Forwarding process (fud) could not receive data from the network, which it needs to do during normal operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_RTSOCK_WRITE_FAILURE

System Log Message Unable to write to routing socket: *error-message*

Description The UDP Forwarding process (fud) could not write to its routing socket for the indicated reason.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_SENDMSG_FAILURE

System Log Message sendmsg() to *destination-address* port *port* on interface *interface-name* rt_inst *routing-instance* failed: *error-message*

Description The UDP Forwarding process (fud) could not send data to the indicated destination port and address via the indicated interface and routing instance, which it needs to do during normal operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_SENDMSG_NOINT_FAILURE

System Log Message sendmsg() to *destination-address* port *port* rt_inst *routing-instance* failed: *error-message*

Description The UDP Forwarding process (fud) could not send data to the indicated destination port and address via the indicated routing instance, which it needs to do during normal operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_SETSOCKOPT_FAILURE

System Log Message setsockopt(*arguments*) failed: *error-message*

Description The UDP Forwarding process (fud) could not set the indicated socket option.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

FUD_SOCKET_FAILURE

System Log Message socket(*arguments*) failed: *error-message*

Description The UDP Forwarding process (fud) could not create a socket.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

Chapter 28

FWAUTH System Log Messages

This chapter describes messages with the FWAUTH prefix. They are generated by the process that authenticates users when they initiate a connection across a firewall.

FWAUTH_FTP_LONG_PASSWORD

System Log Message Authentication for user *username* at *client-address* was denied (long password).

Description The length of the password must not exceed 128 characters.

Type Event: This message reports an event, not an error

Severity info

FWAUTH_FTP_LONG_USERNAME

System Log Message Authentication for user *username* at *client-address* was denied (long username).

Description The length of the username must not exceed 64 characters.

Type Event: This message reports an event, not an error

Severity info

FWAUTH_FTP_USER_AUTH_ACCEPTED

System Log Message User *usernamegroup-name* at *client-address* is accepted.

Description The authenticated user can start accessing protected resources.

Type Event: This message reports an event, not an error

Severity info

FWAUTH_FTP_USER_AUTH_FAIL

System Log Message User *username* at *client-address* is rejected.

Description User authentication failed because the username or password was invalid.

Type Event: This message reports an event, not an error

Severity notice

FWAUTH_HTTP_USER_AUTH_ACCEPTED

System Log Message User *usernamegroup-name* at *client-address* is accepted.

Description The authenticated user can start accessing protected resources.

Type Event: This message reports an event, not an error

Severity info

FWAUTH_HTTP_USER_AUTH_FAIL

System Log Message User *username* at *client-address* is rejected.

Description User authentication failed because the username or password was invalid.

Type Event: This message reports an event, not an error

Severity notice

FWAUTH_TELNET_LONG_PASSWORD

System Log Message Authentication for user *username* at *client-address* was denied (long password).

Description The length of the password must not exceed 128 characters.

Type Event: This message reports an event, not an error

Severity info

FWAUTH_TELNET_LONG_USERNAME

System Log Message Authentication for user *username* at *client-address* was denied (long username).

Description The length of username must not exceed 64 characters.

Type Event: This message reports an event, not an error

Severity info

FWAUTH_TELNET_USER_AUTH_ACCEPTED

System Log Message User *usernamegroup-name* at *client-address* is accepted.

Description The authenticated user can start accessing protected resources

Type Event: This message reports an event, not an error

Severity info

FWAUTH_TELNET_USER_AUTH_FAIL

System Log Message User *username* at *client-address* is rejected.

Description User authentication failed because the username or password was invalid.

Type Event: This message reports an event, not an error

Severity notice

FWAUTH_WEBAUTH_FAIL

System Log Message WebAuth user *username* at *client-address* is rejected/timed out.

Description The provided user credentials are not valid.

Type Event: This message reports an event, not an error

Severity info

FWAUTH_WEBAUTH_SUCCESS

System Log Message WebAuth user *username* at *client-address* is accepted.

Description The authenticated user can start accessing protected resources.

Type Event: This message reports an event, not an error

Severity info

Chapter 29

IDP System Log Messages

This chapter describes messages with the IDP prefix. They are generated by the Intrusion Detection and Prevention (IDP) process.

IDP_ATTACK_LOG_EVENT

System Log Message IDP: at *timestamp*, *message-type* Attack log < *source-address*:*source-port*- > *destination-address*:*destination-port* > for *protocol-name* protocol and service *service-name* by rule *rule-name* of rulebase *rulebase-name* in policy *policy-name*. attack: repeat = *repeat-count*, action = *action*, severity = *severity*, name = *attack-name*, NAT < *nat-source-address*:*nat-source-port*- > *nat-destination-address*:*nat-destination-port* > , time-elapsed = *elapsed-time*, inbytes = *inbound-bytes*, outbytes = *outbound-bytes*, inpackets = *inbound-packets*, outpackets = *outbound-packets*, intf:*source-zone-name*:*source-interface-name*- > *destination-zone-name*:*destination-interface-name*, and misc-message *message*

Description IDP Attack log generated for attack

Type Event: This message reports an event, not an error

Severity info

IDP_DAEMON_INIT_FAILED

System Log Message Aborting...A failure was encountered;*error-message*

Description An attempt to start IDP policy daemon failed because an error was encountered during initialization.

Type Error: An error occurred

Severity error

IDP_INTERNAL_ERROR

System Log Message Encountered an error(*error-message*)

Description IDP daemon encountered an internal error

Type Error: An error occurred

Severity error

IDP_POLICY_COMPILATION_FAILED

System Log Message IDP compilation of policy[*idp-policy*] failed : [*reason*]

Description IDP policy compiler encountered an error while compiling or packaging the policy.Device will continue running the existing IDP policy

Type Event: This message reports an event, not an error

Severity error

IDP_POLICY_LOAD_FAILED

System Log Message IDP policy loading failed policy :[*idp-policy*];detector:*idp-detector*;reason:[*reason*]

Description A compiled and optimized IDP policy could not be loaded into IDP engine. Device will continue running the existing IDP policy.

Type Error: An error occurred

Severity error

IDP_POLICY_LOAD_SUCCEEDED

System Log Message IDP policy[*idp-policy*] and detector[*idp-detector*] loaded successfully.

Description A compiled and optimized IDP policy was loaded successfully into the IDP engine. All subsequent sessions will be processed as per this new IDP policy.

Type Event: This message reports an event, not an error

Severity info

IDP_POLICY_UNLOAD_FAILED

System Log Message Failed to unload IDP policy. reason: *reason*.

Description A running IDP policy could not be unloaded from IDP engine. Device will continue running the IDP policy.

Type Error: An error occurred

Severity error

IDP_POLICY_UNLOAD_SUCCEEDED

System Log Message IDP policy unloaded successfully.

Description A running IDP policy was unloaded successfully from the IDP engine.

Type Event: This message reports an event, not an error

Severity info

IDP_SCHEDULEDUPDATE_START_FAILED

System Log Message Failed to start scheduled update(error:*error-message*)

Description The scheduled IDP security package update failed to start. Device will try it again at the next scheduled time

Type Error: An error occurred

Severity error

IDP_SCHEDULED_UPDATE_STARTED

System Log Message Scheduled update has started(at *timestamp*)

Description The scheduled IDP security package update has started.

Type Event: This message reports an event, not an error

Severity notice

IDP_SECURITY_INSTALL_RESULT

System Log Message security package install result(*status*)

Description IDP background process has returned the security package install result

Type Event: This message reports an event, not an error

Severity notice

IDP_SESSION_LOG_EVENT

System Log Message IDP: at *timestamp*, *event-name* log generated

Description IDP session threshold crossing event

Type Event: This message reports an event, not an error

Severity info

IDP_SIGNATURE_LICENSE_EXPIRED

System Log Message IDP Signagure update license(ID = *feature-id*) has expired

Description IDP signature update license key has expired. Signature update may not work any more.

Type Event: This message reports an event, not an error

Severity warning

Chapter 30

JCS System Log Messages

This chapter describes messages with the JCS prefix. They are generated by the Juniper Control System (jcsd) process.

JCS_BBD_LOAD_FAILURE

System Log Message Blade *slot* load BBD falure: *error-message*

Description The JCS process (jcsd) could not load blade bay data for the specified blade.

Type Error: An error occurred

Severity error

JCS_BBD_LOCAL_MISMATCH

System Log Message Blade *slot* BBD *error-message* mismatch (*expected-value* != *received-value*)

Description The blade bay data retrieved for the specified blade does not match the data loaded during the reboot process. This error usually indicates that blade bay data in the JCS Management Module was changed since the last reboot.

Type Error: An error occurred

Severity error

JCS_BBD_NOT_FOUND

System Log Message Blade *slot* bay data not found

Description Blade bay data was not found for the specified blade.

Type Error: An error occurred

Severity error

JCS_BBD_NOT_VALID

System Log Message Blade *slot* BBD is invalid

Description The blade bay data for the specified blade is invalid.

Type Error: An error occurred

Severity error

JCS_BBD_PARSE_ERROR

System Log Message Blade *slot* bay data parse error - *error-message*

Description The blade bay data for the specified blade did not parse correctly.

Type Error: An error occurred

Severity error

JCS_BBD_PEER_MISMATCH

System Log Message Peer blade *slot* BBD *error-message* mismatch (*expected-value* ! = *received-value*)

Description The blade bay data retrieved for the specified peer blade does not match the data retrieved for the local blade. This error indicates that blade bay data in the JCS Management Module was not configured properly.

Type Error: An error occurred

Severity error

JCS_BBD_SYSTEM_CONFLICT

System Log Message Local BBD *error-message* (*value*) conflicts with blade *slot*

Description The blade bay data retrieved for the local blade conflicts with another blade in the JCS. This error indicates that blade bay data in the JCS Management Module was not configured properly.

Type Error: An error occurred

Severity error

JCS_EXT_LINK_STATE

System Log Message Switch *slot* EXT link state is *state*

Description The JCS process (jcsd) detects a change of state for the external link of the indicated switch module.

Type Event: This message reports an event, not an error

Severity info

JCS_INVALID_BANDWIDTH_ERROR

System Log Message Invalid bandwidth percent (*value*)

Description The specified switch bandwidth is invalid. The bandwidth is defined as a percentage between 1 and 100.

Type Error: An error occurred

Severity error

JCS_KERNEL_RSD_LINK_DOWN

System Log Message Kernel RSD link is DOWN (*error-message*)

Description The JCS process (jcsd) has disabled kernel RSD communcation for the specified reason.

Type Error: An error occurred

Severity error

JCS_KERNEL_RSD_LINK_ENABLED

System Log Message Kernel RSD link is ENABLED (*error-message*)

Description The JCS process (jcsd) has verified the blade bay data and enabled kernel RSD communication.

Type Event: This message reports an event, not an error

Severity info

JCS_MM_COMMUNICATION_ERROR

System Log Message MM communication error (*error-message*)

Description The JCS process (jcsd) could not send an SNMP request to the Management Module because of the indicated error.

Type Error: An error occurred

Severity error

JCS_MM_COMMUNICATION_OK

System Log Message MM communication is OK

Description The JCS process (jcsd) has established a communication link with the Management Module.

Type Event: This message reports an event, not an error

Severity info

JCS_PEER_BLADE_STATE

System Log Message Peer blade *slot* is *state*

Description The JCS process (jcsd) detects a change of state for the indicated blade.

Type Event: This message reports an event, not an error

Severity info

JCS_READ_BANDWIDTH_ERROR

System Log Message Read bandwidth error (*error-code*)

Description The indicated error occured when attempting to read the current switch bandwidth.

Type Error: An error occurred

Severity error

JCS_READ_BBD_ERROR

System Log Message Read blade bay data (error = *error-code*)

Description The indicated error occured when attempting to read the current blade bay data via a sysctl call.

Type Error: An error occurred

Severity error

JCS_RSD_LINK_STATE

System Log Message Switch *slot* RSD link state is *state*

Description The JCS process (jcsd) detects a change of state for the RSD link of the indicated switch module.

Type Event: This message reports an event, not an error

Severity info

JCS_SWITCH_BANDWIDTH_CONFIG

System Log Message Switch *slot* bandwidth *value1* percent (*value2* KBPS)

Description The indicated JCS Switch Module has changed the bandwidth configuration to the specified value.

Type Event: This message reports an event, not an error

Severity info

JCS_SWITCH_COMMUNICATION_ERROR

System Log Message Switch *slot* communication error (*error-message*)

Description The JCS process (jcsd) could not send an SNMP request to the indicated Switch Module because of the indicated error.

Type Error: An error occurred

Severity error

JCS_SWITCH_COMMUNICATION_OK

System Log Message Switch *slot* communication is OK

Description The JCS process (jcsd) has established a communication link with the indicated Switch Module.

Type Event: This message reports an event, not an error

Severity info

Chapter 31

JADE System Log Messages

This chapter describes messages with the JADE prefix. They are generated by the JUNOScript authentication process (jade), which authenticates and checks authorization of client applications using the JUNOScript application programming interface (API).

JADE_ATTRIBUTES_TOO_LONG

System Log Message Attribute number or length in client *junoscript* tag was too large

Description The JUNOScript client passed too many attributes in the initial <junoscript> tag, or the attributes were too long.

Type Error: An error occurred

Severity error

JADE_AUTH_FAILURE

System Log Message Authentication failed for user '*username*' : *error-message*

Description The username or password supplied by the client was incorrect.

Type Error: An error occurred

Severity notice

JADE_AUTH_SUCCESS

System Log Message Authentication succeded for user '*username*'

Description The jade authentication process authenticated the indicated user.

Type Event: This message reports an event, not an error

Severity notice

JADE_EXEC_ERROR

System Log Message CLI xml-mode exec error: *error-message*

Description The JUNOScript authentication process (jade) could not start because of an internal error.

Type Error: An error occurred

Severity error

JADE_PAM_ERROR

System Log Message PAM error: *error-message*

Description The JUNOScript authentication process (jade) could not process the credentials supplied by the client.

Type Error: An error occurred

Severity error

JADE_PAM_NO_LOCAL_USER

System Log Message Unable to get local username from PAM: *error-message*

Description The JUNOScript authentication process (jade) could not obtain a local username while processing the credentials supplied by the client.

Type Error: An error occurred

Severity error

JADE_SOCKET_ERROR

System Log Message Socket operation '*operation*' failed: *error-message*

Description The indicated socket operation, initiated by the JUNOScript authentication process (jade), failed for the indicated reason.

Type Error: An error occurred

Severity error

Chapter 32

JSRPD System Log Messages

This chapter describes messages with the JSRPD prefix. They are generated by the Juniper Services Redundancy Protocol (jsrpd) process, which controls chassis clustering.

JSRPD_DAEMONIZE_FAILED

System Log Message Aborting, unable to run in the background as a daemon: *error-message*

Description The jsrpd process (jsrpd) could not create a version of itself to run in the background as a daemon.

Type Error: An error occurred

Severity emergency

JSRPD_DUPLICATE

System Log Message Another copy of this program is running

Description An attempt to start the jsrpd process (jsrpd) failed because an instance of the process was already running.

Type Error: An error occurred

Severity error

JSRPD_NOT_ROOT

System Log Message Must be run as root

Description The user who attempted to start the JSRP process (jsrpd) was not the root user.

Type Error: An error occurred

Severity error

JSRPD_PID_FILE_LOCK

System Log Message Unable to lock PID file: *error-message*

Description The jsrpd process (jsrpd) attempted to lock the file that records its process ID (PID), which serves to prevent multiple instances of jsrpd from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

JSRPD_PID_FILE_UPDATE

System Log Message Unable to update process PID file: *error-message*

Description The jsrpd process (jsrpd) attempted to update the file that records its process ID (PID), which serves to prevent multiple instances of jsrpd from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

JSRPD_SOCKET_CREATION_FAILURE

System Log Message Socket creation (server) failed unexpectedly *error-message*.

Description The jsrpd process (jsrpd) could not successfully create a socket.

Type Error: An error occurred

Severity error

JSRPD_SOCKET_LISTEN_FAILURE

System Log Message Socket listen (server) failed unexpectedly. *error-message*

Description The jsrpd process (jsrpd) could not successfully listen on a socket.

Type Error: An error occurred

Severity error

JSRPD_SOCKET_RECV_HB_FAILURE

System Log Message Socket reception of heartbeat from failed unexpectedly *error-message*.

Description The jsrpd process (jsrpd) could not successfully receive on a socket.

Type Error: An error occurred

Severity error

JSRPD_USAGE

System Log Message Usage: jsrpd [-C] [-N] [-X] [-d debug-level] [-l] [-v]

Description The jsrpd process (jsrpd) displayed the syntax statement for the 'jsrpd' command because the command was invoked incorrectly.

Type Event: This message reports an event, not an error

Severity error

Chapter 33

KMD System Log Messages

This chapter describes messages with the KMD prefix. They are generated by the key management process (kmd), which provides IP Security (IPSec) authentication services for encryption Physical Interface Cards (PICs).

KMD_CFG_IF_ID_POOL_NOT_FOUND

System Log Message Unable to allocate logical interface for IPSec interface from pool *pool-name*: pool not found

Description The key management process (kmd) maintains pools of logical interfaces for assignment to IP Security (IPSec) interfaces. It could not allocate a logical interface, because it could not access the indicated pool.

Type Error: An error occurred

Severity error

KMD_CFG_IF_ID_POOL_NO_ENTRY

System Log Message Unable to return logical interface *interface-name.interface-unit* to pool *pool-name*: no entry in pool for interface

Description The key management process (kmd) maintains pools of logical interfaces for assignment to IP Security (IPSec) interfaces. It could not return the indicated logical interface to the indicated pool, because there was no entry for the interface in the pool.

Type Error: An error occurred

Severity error

KMD_CFG_IF_ID_POOL_NO_INTERFACE

System Log Message Unable to allocate logical interface for IPSec interface from pool *pool-name*: no interfaces available

Description The key management process (kmd) maintains pools of logical interfaces for assignment to IP Security (IPSec) interfaces. It could not allocate a logical interface, because none were available in the indicated pool.

Type Error: An error occurred

Severity error

KMD_CFG_IF_ID_POOL_RETURN_FAILED

System Log Message Unable to return logical interface to pool *pool-name*: pool not found

Description The key management process (kmd) maintains pools of logical interfaces for assignment to IP Security (IPSec) interfaces. It could not return a logical interface to the indicated pool, because it could not access the pool.

Type Error: An error occurred

Severity error

KMD_DPD_FAILOVER_MANUAL_TUNNEL

System Log Message Tunnel *tunnel-name* did not fail over: it is manual type

Description An IP Security (IPSec) tunnel normally fails over to its backup when the key management process (kmd) detects a dead peer. Failover was not attempted for the indicated tunnel, which is configured as a manual type and so does not support failover.

Type Error: An error occurred

Severity error

KMD_DPD_FAILOVER_MAX_ATTEMPTS

System Log Message Number of failover attempts exceeded limit *count* for tunnel *tunnel-name*

Description An IP Security (IPSec) tunnel fails over to its backup when the key management process (kmd) detects a dead peer. The key management process (kmd) stopped making failover attempts for the indicated tunnel, because the number of attempts exceeded the indicated limit configured for Internet Key Exchange (IKE) Phase 1 negotiations.

Type Error: An error occurred

Severity error

Cause Failover attempts can fail repeatedly if both the primary and backup peers are unreachable during the failover.

KMD_DPD_FAILOVER_NO_ACTIVE_PEER

System Log Message Tunnel *tunnel-name* did not fail over: no active peer configured

Description An IP Security (IPSec) tunnel normally fails over to its backup when the key management process (kmd) detects a dead peer. Failover was not attempted because the configuration for the indicated tunnel does not include information about an active peer.

Type Error: An error occurred

Severity error

KMD_DPD_FAILOVER_NO_BACKUP_PEER

System Log Message Tunnel *tunnel-name* did not fail over: no backup peer configured

Description An IP Security (IPSec) tunnel normally fails over to its backup when the key management process (kmd) detects a dead peer. A failover attempt failed when the kmd process found that the configuration for the indicated tunnel does not include information about a backup peer.

Type Error: An error occurred

Severity error

KMD_DPD_FAILOVER_NO_TUNNEL_CFG

System Log Message Tunnel did not fail over: tunnel configuration not found

Description An IP Security (IPSec) tunnel normally fails over to its backup when the key management process (kmd) detects a dead peer. Failover was not attempted because there was no configuration information for the tunnel.

Type Error: An error occurred

Severity error

KMD_DPD_IKE_SERVER_NOT_FOUND

System Log Message Unable to send DPD reply to remote peer *remote-address*:*remote-port*: no IKE server instance for local peer *local-address*:*local-port*

Description The key management process (kmd) could not retrieve the Internet Key Exchange (IKE) server instance referenced by the indicated local peer (address and port), so it could not reply to the indicated remote peer (address and port) from the local peer.

Type Error: An error occurred

Severity error

KMD_DPD_INVALID_ADDRESS

System Log Message Unable to send DPD reply: local peer *local-address*; remote peer *remote-address*

Description One of the indicated peer addresses (local or remote) was invalid, so the key management process (kmd) could not send a dead peer detection (DPD) reply to the remote peer.

Type Error: An error occurred

Severity error

KMD_DPD_INVALID_SEQUENCE_NUMBER

System Log Message Unable to send DPD reply: remote peer *remote-address*:*remote-port* provided invalid zero sequence number to local peer *local-address*:*local-port*

Description The indicated remote peer (address and port) provided a zero sequence number, which is invalid, to the indicated local peer (address and port). As a result, the key

management process (kmd) could not send a dead peer detection (DPD) reply to the remote peer.

Type Error: An error occurred

Severity error

KMD_DPD_NO_LOCAL_ADDRESS

System Log Message Unable to send DPD hello message from local peer *local-address*/*local-port*: address not found in instance *service-set*

Description The indicated service set did not include an entry for the indicated local peer (address and port), so the key management process (kmd) could not send a dead peer detection (DPD) hello message from that peer.

Type Error: An error occurred

Severity error

KMD_DPD_REMOTE_ADDRESS_CHANGED

System Log Message Remote peer address for tunnel *tunnel-name* changed from *old-address* to *new-address*

Description The remote peer address in the configuration for the indicated tunnel changed to a new value as indicated.

Type Event: This message reports an event, not an error

Severity notice

KMD_DPD_REMOTE_PEER_NOT_FOUND

System Log Message Unable to send DPD reply: DPD entry for remote peer *remote-address*:*remote-port* not found in IKE server instance *service-set*

Description The Internet Key Exchange (IKE) server instance for the indicated service set did not include an entry for the indicated remote peer (address and port), so the key management process (kmd) could not send a dead peer detection (DPD) reply.

Type Error: An error occurred

Severity error

KMD_DPD_UNEXPECTED_IKE_STATUS

System Log Message DPD reply to remote peer *remote-address*:*remote-port* failed with unexpected status *status* for IKE server instance *ike-instance*

Description A dead peer detection (DPD) reply sent to the indicated remote peer (address and port) failed and returned the indicated Internet Key Exchange (IKE) status code for the indicated IKE instance.

Type Error: An error occurred

Severity error

KMD_PM_AUTH_ALGORITHM_INVALID

System Log Message Invalid authentication algorithm *auth-algorithm-id* negotiated in transform *transform-id* for use by *protocol-name* in tunnel *tunnel-name*

Description During Internet Key Exchange (IKE) Phase 2 negotiation of the indicated transform, the indicated authentication algorithm was chosen to be used by the indicated protocol (Authentication Header [AH] or Encapsulating Security Payload [ESP]) for the indicated tunnel. The algorithm is not a valid value, so the associated security association (SA) was not established.

Type Error: An error occurred

Severity error

KMD_PM_DUPLICATE_LIFE_DURATION

System Log Message Duplicate SA life duration value given in Quick Mode notification from *remote-address*:*remote-port*

Description The IKE Quick Mode notification message from the indicated remote gateway and remote port contains duplicate value for life duration. Hence Quick Mode notification payload is dropped.

Type Error: An error occurred

Severity error

KMD_PM_DYNAMIC_SA_INSTALL_FAILED

System Log Message Unable to install dynamic SA for tunnel *tunnel-name*

Description Installation of a dynamic security association (SA) failed for the indicated tunnel during Internet Key Exchange (IKE) Phase 2.

Type Error: An error occurred

Severity error

KMD_PM_ENCRYPTION_INVALID

System Log Message Invalid encryption algorithm negotiated in transform *transform-id* for use by ESP in tunnel *tunnel-name*

Description During Internet Key Exchange (IKE) Phase 2 negotiation of the indicated transform, an encryption algorithm was chosen to be used by the Encapsulating Security Payload (ESP) protocol for the indicated tunnel. The algorithm is not a valid value, so the associated security association (SA) was not installed to the data path.

Type Error: An error occurred

Severity error

KMD_PM_IKE_SERVER_LOOKUP_FAILED

System Log Message No IKE server to connect Phase-1 to *remote-peer*

Description The IKE Phase-1 negotiation with indicated remote gateway address failed because there is no corresponding IKE server running locally.

Type Error: An error occurred

Severity error

KMD_PM_IKE_SERVER_NOT_FOUND

System Log Message Failed to connect to *remote-address*:*remote-port* as there is no IKE server context available in instance *service-set*

Description There is no local IKE server context in the indicated service set, hence failed to send the SPI delete notification request.

Type Error: An error occurred

Severity error

KMD_PM_IKE_SRV_NOT_FOUND_CREATE

System Log Message Local peer *local-address*:*local-port* could not inform remote peer *remote-address*:*remote-port* of SA creation failure: IKE server not found

Description The key management process (kmd) could not connect to the indicated remote peer (address and port), because it could not locate a Internet Key Exchange (IKE) server for the indicated local peer (address and port). As a result, it could not notify the remote peer that a security association (SA) was not created.

Type Error: An error occurred

Severity error

KMD_PM_IKE_SRV_NOT_FOUND_DELETE

System Log Message Unable to notify remote peer *remote-address*:*remote-port* that SPI was deleted: no IKE server for service set *service-set*

Description The indicated service set did not have a local Internet Key Exchange (IKE) server context for the indicated remote peer (address and port). As a result, notification about deletion of a security parameter index (SPI) was not sent.

Type Error: An error occurred

Severity error

KMD_PM_ILLEGAL_REMOTE_GW_ID

System Log Message Aborting Phase-1 negotiation. Cannot initiate negotiation with invalid Phase-1 remote *remote-peer* in instance: *service-set*

Description The specified remote gateway identity is neither an IPv4 address nor an IPv6 address. Hence Phase-1 negotiation can not be started

Type Error: An error occurred

Severity error

KMD_PM_INCONSISTENT_P2_IDS

System Log Message Inconsistent phase-2 (IPsec) identities, local : initiator = *local-initiator* responder = *local-responder* remote : initiator = *remote-initiator* responder = *remote-responder*

Description Initiator and responder identities at the local end are inconsistent with the remote peer's identities. Quick Mode negotiation is aborted.

Type Error: An error occurred

Severity error

KMD_PM_INVALID_LIFE_TYPE

System Log Message Invalid life type *units-type* found in the Quick Mode notification from *remote-address*:*remote-port*

Description The IKE Quick Mode notification message from the indicated remote gateway and remote port contains invalid life type. Second and Kilobytes are the only supported life types currently. Hence Quick Mode notification payload is dropped.

Type Error: An error occurred

Severity error

KMD_PM_KEY_NOT_SUPPORTED

System Log Message Key type *type* not supported

Description The key management process (kmd) retrieved a key of the indicated type during Internet Key Exchange (IKE) Phase 1. The key type is not one of the supported types, which are public/private and preshared.

Type Error: An error occurred

Severity error

KMD_PM_LIFETIME_DUPLICATE

System Log Message Phase 2 lifetime notification message from remote peer *remote-address*:*remote-port* specified duplicate duration

Description During Internet Key Exchange (IKE) Phase 2 negotiation, the indicated remote peer (address and port) sent a lifetime notification message that specified a duplicate value for the security association (SA) lifetime duration. As a result, the key management process (kmd) discarded the notification message.

Type Error: An error occurred

Severity error

KMD_PM_LIFETIME_LENGTH_UNEQUAL

System Log Message Phase 2 lifetime notification message from remote peer *remote-address*:*remote-port* had unequal payload length

Description During Internet Key Exchange (IKE) Phase 2 negotiation, the indicated remote peer (address and port) sent a lifetime notification message with an unequal payload length. As a result, the key management process (kmd) discarded the notification message.

Type Error: An error occurred

Severity error

KMD_PM_LIFETIME_NO_DURATION

System Log Message Phase 2 lifetime notification message from remote peer *remote-address*:*remote-port* did not define duration

Description During Internet Key Exchange (IKE) Phase 2 negotiation, the indicated remote peer (address and port) sent a lifetime notification message that did not specify a duration for the security association (SA) lifetime. As a result, the key management process (kmd) discarded the notification message.

Type Error: An error occurred

Severity error

KMD_PM_LIFETIME_TYPE_UNDEFINED

System Log Message Phase 2 lifetime notification message from remote peer *remote-address*:*remote-port* did not specify life type

Description During Internet Key Exchange (IKE) Phase 2 negotiation, the indicated remote peer (address and port) sent a lifetime notification message that did not specify a life type, making it impossible to determine the lifetime duration for the corresponding security association (SA). As a result, the key management process (kmd) discarded the notification message.

Type Error: An error occurred

Severity error

KMD_PM_LIFETIME_UNITS_INVALID

System Log Message Phase 2 lifetime notification message from remote peer *remote-address*:*remote-port* specified invalid units type *units-type*

Description During Internet Key Exchange (IKE) Phase 2 negotiation, the indicated remote peer (address and port) sent a lifetime notification message that specified the indicated type of units for the security association (SA) lifetime. The type is invalid (the acceptable units are seconds and kilobytes). As a result, the key management process (kmd) discarded the notification message.

Type Error: An error occurred

Severity error

KMD_PM_NEW_GROUP_UNSUPPORTED

System Log Message New Group mode not supported

Description Internet Key Exchange (IKE) New Group mode is not supported, so an attempt to start New Group negotiation failed.

Type Error: An error occurred

Severity error

KMD_PM_NO_LIFETIME

System Log Message Duplicate life time payloads present in the notification from *remote-address*:*remote-port*. Dropping the notification.

Description The IKE Quick Mode notification message from the indicated remote gateway and remote port contains two life type fields and there is no life duration field. Quick Mode notification is being dropped since it has insufficient information about life duration.

Type Error: An error occurred

Severity error

KMD_PM_NO_LIFE_TYPE

System Log Message Quick mode notification from *remote-address*:*remote-port* contains lifetime duration without corresponding SA lifetime payload.

Description The IKE Quick Mode notification message from the indicated remote gateway and remote port does not contain life type, hence existing life duration cannot be interpreted to be of a particular life type. Quick Mode notification payload is dropped.

Type Error: An error occurred

Severity error

KMD_PM_NO_PROPOSAL_FOR_PHASE1

System Log Message Aborting Phase-1negotiation. No proposal found to initiatenegotiation between local:*local-peer* and remote *remote-peer* in instance:*service-set*

Description It is not possible to start the Phase-1 negotiation to the indicated remote gateway because there is no proposal present.

Type Error: An error occurred

Severity error

KMD_PM_NO_SPD_PHASE1_FUNC_PTR

System Log Message Phase-1 SPD handler is not registered in instance:*service-set*

Description Phase-1 negotiation can not be initiated as initialization function failed.

Type Error: An error occurred

Severity error

KMD_PM_P1_POLICY_LOOKUP_FAILURE

System Log Message Policy lookup for Phase-1 [*negotiation-role*] failed for p1_local = *local-peer* p1_remote = *remote-peer*

Description The IKE Phase-1 negotiation with the indicated remote gateway address failed because there is no IKE policy configured for use against the indicated remote gateway.

Type Error: An error occurred

Severity error

KMD_PM_P2_POLICY_LOOKUP_FAILURE

System Log Message Policy lookup for Phase-2 [*negotiation-role*] failed for p1_local = *local-peer* p1_remote = *remote-peer* p2_local = *local-prefix* p2_remote = *remote-prefix*

Description The IKE Phase-2 negotiation with the indicated remote gateway address failed because the traffic selectors proposed by the remote gateway address do not match any of the policies configured for the indicated local gateway address. The proposed traffic selectors are indicated by the Phase-2 local and remote IP prefixes.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_GROUP_UNREADABLE

System Log Message Unable to read group attributes from IKE Phase 1 proposal

Description The key management process (kmd) could not read the information in an Internet Key Exchange (IKE) Phase 1 proposal about the Diffie-Hellman (DH) group to use.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_GROUP_UNSPECIFIED

System Log Message Used DH group 1 because Phase 1 proposal did not specify group

Description The key management process (kmd) assigned Diffie-Hellman (DH) group 1 to an Internet Key Exchange (IKE) Phase 1 proposal because no group was specified.

Type Event: This message reports an event, not an error

Severity error

KMD_PM_PHASE1_IKE_SRV_NOT_FOUND

System Log Message Unable to perform Phase 1 negotiation with remote peer *remote-peer*: no local IKE server

Description The key management process (kmd) could not locate an Internet Key Exchange (IKE) server for the local peer. As a result, IKE Phase 1 negotiation failed with the indicated remote peer.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_NO_IDENTITIES

System Log Message Unable to begin Phase 1 negotiation for local peer *service-set* and remote peer *local-peer* in instance *remote-peer*

Description Internet Key Exchange (IKE) Phase 1 negotiation did not begin, because either the local peer or remote peer was undefined for the indicated service set.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_NO_SPD_HANDLER

System Log Message No Phase 1 SPD handler registered for service set *service-set*

Description A security policy database (SPD) handler is not registered for the indicated service set. As a result, Internet Key Exchange (IKE) Phase 1 negotiation did not begin.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_POLICY_LOOKUP_FAIL

System Log Message Unable to retrieve Phase 1 policy from *negotiation-role* (local peer *local-peer*, remote peer *remote-peer*)

Description The key management process (kmd) could not retrieve a policy from the indicated participant to use during Internet Key Exchange (IKE) Phase 1 negotiation between the indicated local and remote peers.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_POLICY_NOT_FOUND

System Log Message Unable to find policy for Phase 1 negotiation between local peer *local-peer* and remote peer *remote-peer* in service set *service-set*

Description The key management process (kmd) could not retrieve a policy for Internet Key Exchange (IKE) Phase 1 negotiation between the indicated local and remote peers in the indicated service set. As a result, Phase 1 did not begin.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_POLICY_SEARCH_FAIL

System Log Message No ike-policy found for ike-access-profile: *access-profile*, instance:*service-set*

Description The key management process (kmd) could not retrieve the Phase 1 policy referenced by the indicated Internet Key Exchange (IKE) access profile for the indicated dynamic-endpoint service set.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_PROTO_INVALID

System Log Message Phase 1 transform specified invalid protocol *received-value* instead of SSH_IKE_PROTOCOL_ISAKMP (*expected-value*)

Description The indicated protocol in a transform negotiated during Internet Key Exchange (IKE) Phase 1 is not a valid value. The only valid value is the Internet Security Association and Key Management Protocol (ISAKMP). The key management process (kmd) rejected the transform.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_PROTO_NOT_ISAKMP

System Log Message Protocol in IKE Phase 1 proposal was not ISAKMP as expected

Description The protocol in an Internet Key Exchange (IKE) Phase 1 proposal was not the expected value, which is the Internet Security Association and Key Management Protocol (ISAKMP).

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_PROTO_TWICE

System Log Message Phase 1 transform included protocol *protocol-id* twice

Description A transform negotiated during Internet Key Exchange (IKE) Phase 1 specified the indicated protocol twice, which is invalid. The key management process (kmd) rejected the transform.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_TXFORM_INCOMPLETE

System Log Message Phase 1 transform was missing mandatory attributes

Description A transform negotiated during Internet Key Exchange (IKE) Phase 1 did not include values for all attributes. One or more the following was missing: the authentication algorithm, encryption algorithm, or Diffie-Hellman group. The key management process (kmd) rejected the transform.

Type Error: An error occurred

Severity error

KMD_PM_PHASE1_TXFORM_INVALID

System Log Message Phase 1 transform specified invalid transform ID *received-value* instead of *expected-value*

Description The indicated identifier for a transform negotiated during Internet Key Exchange (IKE) Phase 1 is not the indicated expected value. The key management process (kmd) rejected the transform.

Type Error: An error occurred

Severity error

KMD_PM_PHASE2_IDENTITY_MISMATCH

System Log Message Phase 2 identities did not match: local initiator *local-initiator*, responder *local-responder*; remote initiator *remote-initiator*, responder *remote-responder*

Description The indicated initiator and responder identities defined by the local peer did not match the indicated identities defined by the remote peer. The key management process (kmd) canceled Internet Key Exchange (IKE) Phase 2 negotiation.

Type Error: An error occurred

Severity error

KMD_PM_PHASE2_NOTIF_UNKNOWN

System Log Message Unknown Phase 2 notification *notification-name* (type *notification-type*, size *length* bytes) from *remote-address*:*remote-port* for protocol *protocol-id* (SPI(*size*) = *data*)

Description The indicated Internet Key Exchange (IKE) Phase 2 notification message from the indicated remote peer (address and port) is a type that the key management process (kmd) does not support. As a result, the kmd process discarded the message and Phase 2 negotiation failed.

Type Error: An error occurred

Severity error

KMD_PM_PHASE2_POLICY_LOOKUP_FAIL

System Log Message Unable to retrieve policy for Phase 2 from *negotiation-role* (Phase 1 local peer *local-peer*, remote peer *remote-peer*; Phase 2 local peer *local-prefix*, remote peer *remote-prefix*)

Description The key management process (kmd) could not retrieve a policy from the indicated participant to use during Internet Key Exchange (IKE) Phase 2 negotiation for the indicated local and remote peers. The traffic selectors proposed by the remote peer (represented by the indicated Phase 2 IP prefixes) do not match any local peer policies.

Type Error: An error occurred

Severity error

KMD_PM_PHASE2_SELECTOR_UNDEFINED

System Log Message Unable to start Phase 2: No traffic-selector addresses defined for SA *sa-name*

Description The configuration for the indicated security association (SA) did not include the information about local and remote traffic selectors required for Internet Key Exchange (IKE) Phase 2, so that phase did not begin.

Type Error: An error occurred

Severity error

KMD_PM_PROPOSAL_NO_AUTH

System Log Message AH proposal did not define authentication algorithm

Description An Internet Key Exchange (IKE) Phase 2 proposal did not define the authentication algorithm for the Authentication Header (AH) protocol to use. The key management process (kmd) rejected the proposal.

Type Error: An error occurred

Severity error

KMD_PM_PROPOSAL_NO_ENCRYPTION

System Log Message ESP proposal did not define encryption algorithm

Description An Internet Key Exchange (IKE) Phase 2 proposal did not define the encryption algorithm for the Encapsulating Security Payload (ESP) protocol to use. The key management process (kmd) rejected the proposal.

Type Error: An error occurred

Severity error

KMD_PM_PROPOSAL_NO_KEY_LENGTH

System Log Message Phase 2 proposal did not specify length for variable key-length cipher *cipher*

Description An Internet Key Exchange (IKE) Phase 2 proposal did not define the key length for the indicated variable-length cipher. As a result, the key management process (kmd) rejected the proposal.

Type Error: An error occurred

Severity error

KMD_PM_PROPOSAL_NULL_ESP

System Log Message ESP was negotiated with null encryption and authentication

Description Encapsulating Security Payload (ESP) was negotiated as the protocol During Internet Key Exchange (IKE) Phase 2, but no values were negotiated for the authentication and encryption algorithms. As a result, the key management process (kmd) rejected the transform.

Type Error: An error occurred

Severity error

KMD_PM_PROPOSAL_PROTOCOL_INVALID

System Log Message Protocol *protocol-id* in Phase 2 proposal was invalid (was not AH or ESP)

Description An Internet Key Exchange (IKE) Phase 2 proposal specified the indicated protocol, which is invalid. The acceptable protocols as Authentication Header (AH) and Encapsulating Security Payload (ESP). The key management process (kmd) rejected the proposal.

Type Error: An error occurred

Severity error

KMD_PM_PROTO_INVALID

System Log Message Invalid protocol *protocol-id* was negotiated for SA *sa-name*

Description During Internet Key Exchange (IKE) Phase 2, the indicated protocol was chosen for the indicated security association (SA). It is not a valid value, so the SA was not established.

Type Error: An error occurred

Severity error

KMD_PM_PROTO_IPCOMP_UNSUPPORTED

System Log Message Unsupported IPComp protocol was negotiated for SA *sa-name*

Description During Internet Key Exchange (IKE) Phase 2, the IP Payload Compression Protocol (IPComp) was chosen for the indicated security association (SA). IPComp is not supported, so the SA was not established.

Type Error: An error occurred

Severity error

KMD_PM_PROTO_ISAKMP_RESV_UNSUPP

System Log Message Unsupported protocol ISAKMP or RESERVED was negotiated for SA *sa-name*

Description During Internet Key Exchange (IKE) Phase 2, either Internet Security Association and Key Management Protocol (ISAKMP) or the value RESERVED was chosen as the protocol for the indicated security association (SA). They are not supported values, so the SA was not established.

Type Error: An error occurred

Severity error

KMD_PM_PROTO_NOT_NEGOTIATED

System Log Message No protocol negotiated for SA *sa-name*

Description While verifying the results of Internet Key Exchange (IKE) Phase 2, the key management process (kmd) determined that no protocol was negotiated for the indicated security association (SA). The SA was not established.

Type Error: An error occurred

Severity error

KMD_PM_REMOTE_PEER_INVALID

System Log Message Phase 1 negotiation failed: remote address *remote-peer* in instance *service-set* is invalid

Description Internet Key Exchange (IKE) Phase 1 negotiation failed because the indicated remote peer address in the indicated service set is not a valid IP version 4 (IPv4) or IP version 6 (IPv6) address.

Type Error: An error occurred

Severity error

KMD_PM_SA_CFG_NOT_FOUND

System Log Message Unable to install negotiated Phase 2 values: SA *sa-name* configuration not found

Description The key management process (kmd) could not retrieve configuration information for the indicated security association (SA), and so could not record the values that were negotiated for the SA during Internet Key Exchange (IKE) Phase 2. The SA was not established.

Type Error: An error occurred

Severity error

KMD_PM_SA_DELETE_REJECT

System Log Message Rejected SA deletion request for service set *service-set*: SPI size (*size*) is not 4 (local peer *local-address*:*local-port*, remote peer *remote-address*:*remote-port*)

Description The key management process (kmd) discarded a message that requested deletion of a security association (SA) between the indicated local peer (address and port) and remote peer (address and port), because the indicated size of the associated Security Parameter Index (SPI) was not as expected. As a result, the SA was not deleted.

Type Error: An error occurred

Severity error

KMD_PM_SA_INDEX_GEN_FAILED

System Log Message Unable to generate pair index for SA *sa-name* in service set *service-set*

Description The key management process (kmd) could not generate a pair index for the indicated security association (SA) in the indicated service set. The kmd process canceled Internet Key Exchange (IKE) Phase 2 negotiation.

Type Error: An error occurred

Severity error

KMD_PM_SA_PEER_ABSENT

System Log Message No active peer found in tunnel configuration block *sa-name*

Description Failed to find active peer information in the tunnel configuration block. Hence unable to send SA delete notifications to the peer.

Type Error: An error occurred

Severity error

KMD_PM_SA_PEER_NOT_FOUND

System Log Message Unable to find active peer for SA *sa-name*

Description The key management process (kmd) could not retrieve information about an active peer from the configuration for the indicated security association (SA). As a result, it could not notify peers that an SA was deleted.

Type Error: An error occurred

Severity error

KMD_PM_SPI_DELETE_REJECT

System Log Message IKE Phase-2 delete:In instance *service-set* rejecting request to delete SPI size *size*u != 4 Local gateway *local-address*:*local-port*, Remote gateway *remote-address*:*remote-port*

Description The SPI size in the delete notification is invalid. Hence delete request is rejected. Quick Mode notification payload is dropped.

Type Error: An error occurred

Severity error

KMD_PM_UNEQUAL_PAYLOAD_LENGTH

System Log Message Inconsistent payload lengths in Quick Mode responder life time notification from *remote-address*:*remote-port*

Description IKE Quick Mode notification is dropped because of unequal payload length received in the message.

Type Error: An error occurred

Severity error

KMD_PM_UNINITIALISE_ERROR

System Log Message Invalid policy managerhandle to uninitialize *service-set*

Description Failed to uninitialize the Policy manager object while deleting the indicated service set.

Type Error: An error occurred

Severity error

KMD_PM_UNINITIALIZE_FAILED

System Log Message Unable to uninitialize service set *service-set*: invalid policy manager handle

Description The key management process could not delete the indicated service set, because lack of a valid handle prevented the kmd process from uninitializing the policy manager object for the service set.

Type Error: An error occurred

Severity error

KMD_PM_UNKNOWN_P1_IDENTITIES

System Log Message Failed to initiate the Phase-1 negotiation for local:*local-peer* and remote:*remote-peer* in instance:*service-set*

Description Phase-1 negotiation can not be started because either the local gateway identity or the remote gateway identity is unknown.

Type Error: An error occurred

Severity error

KMD_PM_UNKNOWN_PHASE2_ENTITIES

System Log Message No Phase-2 entities present in tunnel configuration block *sa-name*

Description Unable to initiate Phase-2 negotiation because of unknown local and remote traffic selectors in the indicated security association configuration block. For Adaptive Service PIC, the security association configuratin block refers to the tunnel configured under a service set with a given rule name and term name.

Type Error: An error occurred

Severity error

KMD_PM_UNKNOWN_QM_NOTIFICATION

System Log Message Unknown Quick mode notification *notification-name* (*notification-type*) (size *length*ubytes) from *remote-address*:*remote-port* for protocol = *protocol-id*d spi(*size*u) = *data*

Description The notification message sent by the indicated remote gateway and remote port is not recognized. Hence Quick Mode notification payload is dropped.

Type Error: An error occurred

Severity error

KMD_PM_UNSUPPORTED_KEY

System Log Message Key type = *type*, not supported

Description The specified key type is unsupported. Public/Private and Pre-shared key are are the only types supported presently.

Type Error: An error occurred

Severity error

KMD_PM_UNSUPPORTED_MODE

System Log Message New group mode not supported currently

Description The IKE New Group mode negotiations failed, because this is not a supported feature currently.

Type Error: An error occurred

Severity error

KMD_SNMP_EXTRA_RESPONSE

System Log Message PIC *pic-slot* sent additional response after reply to SNMP query: *error-message*

Description The indicated Physical Interface Card (PIC) sent an additional unexpected message after it responded to a request from the key management process (kmd) for Simple Network Management Protocol (SNMP) statistics about IP Security (IPSec) security associations (SAs). As a result, the kmd process discarded the initial response.

Type Error: An error occurred

Severity error

KMD_SNMP_FATAL_ERROR

System Log Message Fatal SNMP error occurred: *error-message*

Description The key management process (kmd) could not retrieve Simple Network Management Protocol (SNMP) statistics about IP Security (IPSec) security associations (SAs), because the indicated fatal SNMP error occurred.

Type Error: An error occurred

Severity error

KMD_SNMP_IKE_SERVER_NOT_FOUND

System Log Message Unable to fulfill SNMP request: could not fetch IKE server context for service set *service-set*

Description The key management process (kmd) could not retrieve the Internet Key Exchange (IKE) server context for the indicated service set. As a result, it could not process a request for Simple Network Management Protocol (SNMP) statistics.

Type Error: An error occurred

Severity error

KMD_SNMP_MALLOC_FAILED

System Log Message Unable to allocate memory for reply buffer; SNMP query to PIC *pic-slot* failed

Description The key management process (kmd) could not allocate memory for the buffer it uses to store Simple Network Management Protocol (SNMP) statistics about IP Security (IPSec) security associations (SAs). As a result, it could not retrieve statistics from the indicated Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

KMD_SNMP_PIC_CONNECTION_FAILED

System Log Message Unable to connect to PIC *pic-slot*; SNMP query failed

Description The key management process (kmd) could not open a connection to the indicated Physical Interface Card (PIC). As a result, it could not retrieve Simple Network Management Protocol (SNMP) statistics about IP Security (IPSec) security associations (SAs).

Type Error: An error occurred

Severity error

KMD_SNMP_PIC_NO_RESPONSE

System Log Message PIC *pic-slot* did not respond to SNMP query: *error-message*

Description The indicated Physical Interface Card (PIC) did not respond to a request from the key management process (kmd) for Simple Network Management Protocol (SNMP) statistics about IP Security (IPSec) security associations (SAs).

Type Error: An error occurred

Severity error

KMD_SNMP_PIC_SLOT_NOT_FOUND

System Log Message Unable to retrieve slot information for PIC *pic-slot*; SNMP query failed

Description The key management process (kmd) could not retrieve information about the slot housing the indicated Physical Interface Card (PIC). As a result, it could not retrieve Simple Network Management Protocol (SNMP) statistics about IP Security (IPSec) security associations (SAs) from the PIC.

Type Error: An error occurred

Severity error

KMD_VPN_DFBIT_STATUS_MSG

System Log Message The DF-BIT for VPN *vpn-name* has been set to *argument*.

Description VPN DF bit status has been set.

Type Event: This message reports an event, not an error

Severity info

KMD_VPN_DOWN_ALARM_USER

System Log Message VPN *vpn-name* from *remote-address* is down.

Description Notifiication to user that VPN monitor detects IPSec SA is down.

Type Event: This message reports an event, not an error

Severity info

KMD_VPN_UP_ALARM_USER

System Log Message VPN *vpn-name* from *remote-address* is up.

Description Notifiication to user that VPN monitor detects IPSec SA is up.

Type Event: This message reports an event, not an error

Severity info

Chapter 34

L2ALD System Log Messages

This chapter describes messages with the L2ALD prefix. They are generated by the Layer 2 address learning process (l2ald), which supports the dynamic acquisition of information about media access control (MAC) addresses in a Layer 2 bridge environment.

L2ALD_GENCFG_OP_FAILED

System Log Message Unable to complete gencfg operation *operation* (major *type*, minor *subtype*): *error-message*

Description The Layer 2 address learning process (l2ald) could not send Layer 2 forwarding-related information to the Packet Forwarding Engines, because the indicated operation failed during configuration generation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2ALD_IPC_MESSAGE_ERROR

System Log Message Message (type *message-type*, subtype *message-subtype*, opcode *message-opcode*) received with error *error-message*

Description The Layer 2 address learning process (l2ald) detected an error in an interprocess communication (IPC) message with the indicated characteristics.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2ALD_IPC_MESSAGE_INVALID

System Log Message Invalid message received (message type *message*, subtype *message-type*): *message-subtype*

Description The Layer 2 address learning process (l2ald) received a message with the indicated characteristics. The message was invalid for the indicated reason.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2ALD_IPC_MESSAGE_SEND_FAILED

System Log Message Unable to send IPC message to *peer-name identifier*

Description The Layer 2 address learning process (l2ald) could not send an interprocess communication (IPC) message to the indicated Layer 2 peer.

Type Error: An error occurred

Severity warning

Action Contact your technical support representative.

L2ALD_IPC_PIPE_WRITE_ERROR

System Log Message Unable to write on pipe: *error-message*

Description The Layer 2 address learning process (l2ald) could not write to an interprocess communication (IPC) pipe for the indicated reason.

Type Error: An error occurred

Severity error

Cause One possible reason is that there was no reader for the pipe.

Action Contact your technical support representative.

L2ALD_MAC_LIMIT_REACHED_BD

System Log Message Limit on learned MAC addresses reached for routing instance '*routing-instance*', domain '*bridge-domain*:*vlan-id*'; current count is *count*

Description The Layer 2 address learning process (l2ald) stopped adding addresses to the MAC address table that were learned by interfaces in the indicated bridging domain, because the indicated count of learned addresses exceeds the configured or default limit for the bridge-domain.

Type Event: This message reports an event, not an error

Severity error

Action Increase the limit on addresses learned by interfaces in the bridge domain, by increasing the value of the 'interface-mac-limit' statement at the [edit routing-instances <routing-instance-name> bridge-domains <bridge-domain-name> bridge-options] hierarchy level.

L2ALD_MAC_LIMIT_REACHED_GLOBAL

System Log Message Global limit on learned MAC addresses reached; current count is *count*

Description The Layer 2 address learning process (l2ald) stopped adding addresses to the MAC address table, because the indicated count of learned addresses exceeds the limit for the router.

Type Event: This message reports an event, not an error

Severity error

Action Increase the limit on addresses learned by the interfaces on the router by increasing the value of the 'global-mac-limit' statement at the [edit protocols l2-learning] hierarchy level.

L2ALD_MAC_LIMIT_REACHED_IF

System Log Message Limit on learned MAC addresses reached for *interface-name*; current count is *count*

Description The Layer 2 address learning process (l2ald) stopped adding addresses to the MAC address table that were learned by the indicated interface, because the indicated count of learned addresses exceeds the limit configured for the interface.

Type Event: This message reports an event, not an error

Severity error

Action Increase the limit on addresses learned by the interface by increasing the value of the 'interface-mac-limit' statement at the appropriate location under the [edit routing-instances <routing-instance-name> bridge-domains <bridge-domain-name> bridge-options] or the [edit routing-instances <routing-instance-name> protocols vpls] hierarchy level.

L2ALD_MAC_LIMIT_REACHED_IFBD

System Log Message Limit on learned MAC addresses reached for *interface-name*; current count is *count*

Description The Layer 2 address learning process (l2ald) stopped adding addresses to the MAC address table that were learned by the indicated interface:vlan-id, because the indicated count of learned addresses exceeds the limit configured for the interface:vlan-id.

Type Event: This message reports an event, not an error

Severity error

Action Increase the limit on addresses learned by the interface by increasing the value of the 'interface-mac-limit' statement at the appropriate location under the [edit routing-instances <routing-instance-name> bridge-domains <bridge-domain-name> bridge-options] or the [edit routing-instances <routing-instance-name> protocols vpls] hierarchy level.

L2ALD_MAC_LIMIT_REACHED_RTT

System Log Message Limit on learned MAC addresses reached for routing instance '*routing-instance*'; current count is *count*

Description The Layer 2 address learning process (l2ald) stopped adding addresses to the MAC address table that were learned by interfaces in the indicated routing instance,

because the indicated count of learned addresses exceeds the configured or default limit for the routing-instance.

Type Event: This message reports an event, not an error

Severity error

Action Increase the limit on addresses learned by interfaces in the routing-instance, by increasing the value of the 'interface-mac-limit' statement at the [edit routing-instances <routing-instance-name> protocol l2-learning] or the [edit routing-instances <routing-instance-name> protocols vpls] hierarchy level.

L2ALD_MAC_LIMIT_RESET_BD

System Log Message Resumed adding MAC addresses learned from routing instance '*routing-instance*', domain '*bridge-domain*:*vlan-id*'; current count is *count*

Description The Layer 2 address learning process (l2ald) resumed adding addresses to the MAC address table that were learned by interfaces in the indicated bridging domain, because the indicated count of learned addresses no longer exceeds the limit configured for the domain.

Type Event: This message reports an event, not an error

Severity error

Cause The probable reason that the count of addresses went below the limit is that addresses in the table reached the age limit and were removed.

L2ALD_MAC_LIMIT_RESET_GLOBAL

System Log Message Resumed adding MAC addresses for router; current count is *count*

Description The Layer 2 address learning process (l2ald) resumed adding addresses to the MAC address table, because the indicated count of learned addresses no longer exceeds the configured limit.

Type Event: This message reports an event, not an error

Severity error

Cause The probable reason that the count of addresses went below the limit is that addresses in the table reached the age limit and were removed.

L2ALD_MAC_LIMIT_RESET_IF

System Log Message Resumed adding MAC addresses learned by *interface-name*; current count is *count*

Description The Layer 2 address learning process (l2ald) resumed adding addresses to the MAC address table that were learned by the indicated interface, because the indicated count of learned addresses no longer exceeds the limit configured for the interface.

Type Event: This message reports an event, not an error

Severity error

Cause The probable reason that the count of addresses went below the limit is that addresses in the table reached the age limit and were removed.

L2ALD_MAC_LIMIT_RESET_RTT

System Log Message Resumed adding MAC addresses learned from routing instance '*routing-instance*'; current count is *count*

Description The Layer 2 address learning process (l2ald) resumed adding addresses to the MAC address table that were learned by interfaces in the indicated bridging domain, because the indicated count of learned addresses no longer exceeds the limit configured for the instance.

Type Event: This message reports an event, not an error

Severity error

Cause The probable reason that the count of addresses went below the limit is that addresses in the table reached the age limit and were removed.

L2ALD_MAC_MOVE_NOTIFICATION

System Log Message MAC Moves detected in the system

Description When the same MAC address is learned on a different interface, or on the same interface but different unit number, it is considered to be a MAC move. When this happens frequently for a specific time duration, a notification is sent.

Type Event: This message reports an event, not an error

Severity warning

Cause The probable reason for mac moves is the loops in the topology or some kind of misconfiguration.

L2ALD_MALLOC_FAILED

System Log Message Unable to allocate memory: *error-message*

Description The Layer 2 address learning process (l2ald) could not allocate memory while creating a data structure.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2ALD_MANAGER_CONNECT

System Log Message Unable to create pipe to Layer 2 address-learning manager: *error-message*

Description The Layer 2 address learning process (l2ald) could not open a pipe for interprocess communication (IPC) with a Layer 2 address-learning manager process.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2ALD_NAME_LENGTH_IF_DEVICE

System Log Message Unable to add interface device *interface-name*; name exceeds limit of *length* characters

Description The Layer 2 address learning process (l2ald) did not add an entry for the indicated interface device to the interface table, because its name exceeds the indicated limit on the number of characters.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2ALD_NAME_LENGTH_IF_FAMILY

System Log Message Unable to add interface family *interface-family*; name exceeds limit of *length* characters

Description The Layer 2 address learning process (l2ald) did not add an entry for the indicated interface family to the interface table, because its name exceeds the indicated limit on the number of characters.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2ALD_NAME_LENGTH_IF_LOGICAL

System Log Message Unable to add logical interface *interface-name*; name exceeds limit of *length* characters

Description The Layer 2 address learning process (l2ald) did not add an entry for the indicated logical interface to the interface table, because its name exceeds the indicated limit on the number of characters.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

Chapter 35

L2CPD System Log Messages

This chapter describes messages with the L2CPD prefix. They are generated by the Layer 2 Control Protocol process (l2cpd), which supports the transmission of control messages for Layer 2 spanning tree protocols in a Layer 2 bridge environment.

L2CPD_ASSERT

System Log Message Assertion failed for *executable-name* (PID *pid*) at line *line-number* in file '*source-filename*': *message*

Description The source code for the Layer 2 Control Protocol process (l2cpd) includes internal self-consistency tests. The l2cpd process with the indicated executable name and process ID (PID) terminated because the indicated test failed at the indicated line number in the indicated source file. The process created a diagnostic core file for analysis by technical support personnel.

Type Error: An error occurred

Severity error

Cause Messages that immediately follow this message in the system log might provide information about possible causes.

Action Contact a technical support representative, and be ready to provide the list of messages and the diagnostic core file, if requested.

L2CPD_ASSERT_SOFT

System Log Message Assertion failed for *executable-name* (PID *pid*) at line *line-number* in file '*source-filename*' (*message*); process continued running

Description The source code for the Layer 2 Control Protocol process (l2cpd) includes internal self-consistency tests. The l2cpd process with the indicated executable name and process ID (PID) terminated because the indicated type of check failed at the indicated line number in the indicated source file. The process continued to run, but created a diagnostic core file for analysis by technical support personnel.

Type Error: An error occurred

Severity error

Cause Messages that immediately follow this message in the system log might provide information about possible causes.

Action Contact a technical support representative, and be ready to provide the list of messages and the diagnostic core file, if requested.

L2CPD_EXIT

System Log Message l2cpd process with PID *pid* exited (was using executable *executable-name*, version *version* built by *builder* on *date*); caller was *address*

Description The Layer 2 Control Protocol process (l2cpd) exited. The process had the indicated process ID (PID) and was using an executable with the indicated name, version, and other characteristics.

Type Event: This message reports an event, not an error

Severity notice

Cause Either a system resource was unavailable, the l2cpd process could not interpret an error, or the indicated user (referred to as a 'caller') terminated the process.

L2CPD_KERNEL_VERSION

System Log Message Kernel version (*kernel-version*) of routing sockets was not required version (*l2cpd-version*)

Description The Layer 2 Control Protocol process (l2cpd) determined that the indicated version of routing sockets, which the kernel supports, is not the version that it requires.

Type Error: An error occurred

Severity error

Action Upgrade the kernel package.

L2CPD_KERNEL_VERSION_OLD

System Log Message Kernel version (*kernel-version*) of routing socket message type *message-type* is older than the required version (*l2cpd-version*)

Description The Layer 2 Control Protocol process (l2cpd) determined that the kernel supports an indicated older version of the indicated routing socket message type than it requires.

Type Error: An error occurred

Severity error

Action Upgrade the kernel package.

L2CPD_KERNEL_VERSION_UNSUPP

System Log Message Kernel version of routing socket message type '*message-type*' was not required version (*l2cpd-version*)

Description The Layer 2 Control Protocol process (l2cpd) determined that the kernel does not support the version of the indicated routing socket message type that it requires.

Type Error: An error occurred

Severity error

Action Upgrade the kernel package.

L2CPD_MEMORY_EXCESSIVE

System Log Message Using *size* KB of memory, *percentage-value* percent of available

Description The Layer 2 Control Protocol process (l2cpd) was using the indicated amount and percentage of Routing Engine memory, which is considered excessive.

Type Error: An error occurred

Severity error

Cause Either the l2cpd process is leaking memory or the use of system resources is excessive. Possible causes include misconfigured routing filters or a very complex configured network topology.

Action Increase the amount of RAM in the Routing Engine.

L2CPD_MGMT_TIMEOUT

System Log Message Peer *peer-name* timed out

Description The Layer 2 Control Protocol process (l2cpd) did not receive input from the indicated management peer within the timeout period.

Type Error: An error occurred

Severity warning

Cause Messages that immediately follow this message in the system log might provide information about possible causes.

L2CPD_MIRROR_ERROR

System Log Message Unable to establish mirror connection between Routing Engines: *error-message*

Description The Layer 2 Control Protocol process (l2cpd) could not establish the mirror connection (which supports nonstop routing) between the master and backup Routing Engines.

Type Error: An error occurred

Severity warning

Cause The master and backup Routing Engines are running incompatible versions of the JUNOS software.

Action Update the JUNOS software to compatible versions on the master and backup Routing Engines.

L2CPD_MIRROR_VERSION_MISMATCH

System Log Message Mirror version (*master-version*) on master Routing Engine*master-is-local* is not compatible with version (*standby-version*) on backup*standby-is-local*

Description While trying to establish the mirror connection (which supports nonstop routing) between the master and backup Routing Engines, the Layer 2 Control Protocol process (l2cpd) determined that the versions of JUNOS software on the Routing Engines were incompatible.

Type Error: An error occurred

Severity warning

Action Update the JUNOS software to compatible versions on the master and backup Routing Engines.

L2CPD_PPM_READ_ERROR

System Log Message Read error on pipe from ppmd: *reason* (*error-message*)

Description The Layer 2 Control Protocol process (l2cpd) could not read a message available on the read pipe from the periodic packet management process (ppmd).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2CPD_PPM_WRITE_ERROR

System Log Message *function-name*: write error on pipe to ppmd (*error-message*)

Description The Layer 2 Control Protocol process (l2cpd) could not write a message on the pipe to the periodic packet management process (ppmd).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

L2CPD_RUNTIME_MODULE

System Log Message *function-name*: runtime was excessive (*time*) during *action* of *module*

Description The indicated operation on the indicated submodule of the Layer 2 Control Protocol process (l2cpd) ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The message was logged because task accounting is enabled. The function might be implemented inefficiently.

L2CPD_RUNTIME_OPERATION

System Log Message *function-name*: runtime was excessive (*time*) during *action* of *module*

Description The indicated operation on the indicated submodule of the Layer 2 Control Protocol process (l2cpd) ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The message was logged because task accounting is enabled. The function might be implemented inefficiently.

L2CPD_RUNTIME_TASK

System Log Message *function-name*: runtime was excessive (*total-time* [*user-time* user, *system-time* system]) doing *action*

Description While performing the indicated operation, the indicated function in the Layer 2 Control Protocol process (l2cpd) ran uninterrupted for the indicated period of time (the sum of the indicated user and system times), which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The message was logged because task accounting is enabled. The function might be implemented inefficiently.

L2CPD_RUNTIME_TOTAL

System Log Message *function-name*: runtime was excessive (total of *time* in *count* callbacks) after *action* of *module*

Description After the indicated operation on the indicated submodule of the Layer 2 Control Protocol process (l2cpd), several functions ran uninterrupted in the indicated number of callbacks for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The message was logged because task accounting is enabled. The function might be implemented inefficiently.

L2CPD_TASK_BEGIN

System Log Message l2cpd process started (version *l2cpd-version* built on *date* by *builder*)

Description The Layer 2 Control Protocol process (l2cpd) started. It was assigned the indicated process ID (PID) and was using an executable with the indicated name, version, and build date.

Type Event: This message reports an event, not an error

Severity notice

L2CPD_TASK_CHILD_KILLED

System Log Message Child process '*task-name*' terminated by SIG*signal-name core-dump-status*

Description While a child process of the Layer 2 Control Protocol process (l2cpd) was performing the indicated operation, it terminated in response to the indicated signal.

Type Event: This message reports an event, not an error

Severity error

L2CPD_TASK_CHILD_STOPPED

System Log Message Child process '*task-name*' stopped by SIG*signal-name*

Description While a child process of the Layer 2 Control Protocol process (l2cpd) was performing the indicated operation, it stopped in response to the indicated signal.

Type Event: This message reports an event, not an error

Severity error

L2CPD_TASK_FORK

System Log Message Unable to fork *task-name*: *error-message*

Description The Layer 2 Control Protocol process (l2cpd) could not create the indicated child process.

Type Error: An error occurred

Severity error

L2CPD_TASK_GETWD

System Log Message getwd() failed for *error-message*

Description The Layer 2 Control Protocol process (l2cpd) invoked the getwd() system call, which failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources needed to fulfill the request. The l2cpd process continued operating.

L2CPD_TASK_MASTERSHIP

System Log Message Assumed mastership

Description The Layer 2 Control Protocol process (l2cpd) became active when the Routing Engine on which it was running assumed mastership.

Type Event: This message reports an event, not an error

Severity info

L2CPD_TASK_NO_REINIT

System Log Message Unable to reinitialize

Description The Layer 2 Control Protocol process (l2cpd) did not reinitialize as requested, because it was running in a state that did not allow reconfiguration.

Type Error: An error occurred

Severity error

L2CPD_TASK_PID_CLOSE

System Log Message Unable to close and remove PID file *filename*: *error-message*

Description The Layer 2 Control Protocol process (l2cpd) could not close and remove the file that records its process ID (PID), which serves to prevent multiple instances of the l2cpd process from running simultaneously.

Type Error: An error occurred

Severity error

L2CPD_TASK_PID_LOCK

System Log Message flock(*filename*, LOCK_EX): *error-message*

Description The Layer 2 Control Protocol process (l2cpd) could not lock the file that records its process ID (PID), which serves to prevent multiple instances of the l2cpd process from running simultaneously.

Type Error: An error occurred

Severity error

L2CPD_TASK_PID_WRITE

System Log Message Unable to write to PID file *filename*: *error-message*

Description The Layer 2 Control Protocol process (l2cpd) could not write to the file that records its process ID (PID), which serves to prevent multiple instances of the l2cpd process from running simultaneously.

Type Error: An error occurred

Severity error

L2CPD_TASK_REINIT

System Log Message Reinitialized

Description The Layer 2 Control Protocol process (l2cpd) reinitialized.

Type Event: This message reports an event, not an error

Severity info

L2CPD_TASK_SIGNAL_IGNORE

System Log Message Unable to register SIG*signal-name* to be ignored: *error-message*

Description The Layer 2 Control Protocol process (l2cpd) informed the kernel that it wished to ignore the indicated signal, but the kernel did not process the request.

Type Error: An error occurred

Severity error

L2CPD_TERMINATE_ACTIVE

System Log Message Exited with active tasks: *task-name*

Description After receiving multiple termination requests, the Layer 2 Control Protocol process (l2cpd) exited without performing the indicated cleanup tasks.

Type Event: This message reports an event, not an error

Severity notice

L2CPD_TERMINATE_SIGNAL

System Log Message Exited after receiving termination signal *signal-name*

Description In response to the indicated termination request, the Layer 2 Control Protocol process (l2cpd) terminated adjacencies with neighbors and shut down.

Type Event: This message reports an event, not an error

Severity notice

L2CPD_TRACE_FAILED

System Log Message Unable to write to trace file *filename*

Description The Layer 2 Control Protocol process (l2cpd) could not write to the indicated trace file, and stopped attempting to do so. The next commit of the configuration database will reenable tracing.

Type Event: This message reports an event, not an error

Severity error

L2CPD_XSTP_SHUTDOWN_FAILED

System Log Message Unable to shut down *error-message* module

Description The Layer 2 Control Protocol process (l2cpd) could not shut down the indicated Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP) module.

Type Error: An error occurred

Severity error

Chapter 36

L2TPD System Log Messages

This chapter describes messages with the L2TPD prefix. They are generated by the Layer 2 Tunneling Protocol (L2TP) process (l2tpd), which provides services that enable tunneling of Point-to-Point Protocol (PPP) sessions across a Layer 3 IP network.

L2TPD_COS_PROFILE_ADD

System Log Message Unable to add CoS profile *profile-name* (L2TP tunnel *tunnel-id*, session *session-id*): *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add the indicated class-of-service (CoS) profile to the indicated session on the indicated tunnel, which is associated with a user.

Type Error: An error occurred

Severity error

Action Remove the CoS profile from the RADIUS database or contact your technical support representative.

L2TPD_COS_PROFILE_DELETE

System Log Message Unable to delete CoS profile (L2TP tunnel *tunnel-id*, session *session-id*): *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete a class-of-service (CoS) profile from the indicated session on the indicated tunnel, which is associated with a user.

Type Error: An error occurred

Severity error

Action Remove the CoS profile from the RADIUS database or contact your technical support representative.

L2TPD_DB_ADD_FAILED

System Log Message Unable to add node for *node-name* to internal database

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add the indicated node to the in-memory database.

Type Error: An error occurred

Severity error

L2TPD_DB_DELETE_FAILED

System Log Message Unable to delete node for *node-name* from internal database

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not delete the indicated node to the in-memory database.

Type Error: An error occurred

Severity error

L2TPD_DB_INIT_FAILED

System Log Message Unable to initialize root node *object-name* in internal database: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not initialize the root node for the indicated object in the in-memory database.

Type Error: An error occurred

Severity error

L2TPD_DB_TUN_GRP_ALLOC_FAILED

System Log Message Unable to allocate memory for tunnel group

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate memory for the data structure used to record tunnel group information.

Type Error: An error occurred

Severity error

L2TPD_DEFAULT_PROTO_CREATE_FAIL

System Log Message Unable to create default L2TP module

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create a default L2TP module.

Type Error: An error occurred

Severity error

L2TPD_EVLIB_CREATE_FAILED

System Log Message Unable to create event context: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create a context for handling asynchronous events.

Type Error: An error occurred

Severity emergency

L2TPD_EVLIB_FD_DEREGISTER_FAILED

System Log Message Unable to deregister file descriptor: not registered

Description The Layer 2 Tunneling Protocol process (l2tpd) could not deregister a file descriptor, because it did not exist.

Type Error: An error occurred

Severity error

L2TPD_EVLIB_FD_DESELECT_FAILED

System Log Message Unable to deselect file descriptor: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not deselect a file descriptor.

Type Error: An error occurred

Severity error

L2TPD_EVLIB_FD_NOT_REGISTERED

System Log Message No file descriptor registered

Description The Layer 2 Tunneling Protocol process (l2tpd) could not find a registered file descriptor while attempting to set an event mask.

Type Error: An error occurred

Severity error

L2TPD_EVLIB_FD_SELECT_FAILED

System Log Message Unable to select file descriptor for events *event-id*: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not select the file descriptor for the indicated events.

Type Error: An error occurred

Severity error

L2TPD_EVLIB_TIMER_CLEAR_FAILED

System Log Message Unable to clear event timer: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not clear an event timer for the indicated reason.

Type Error: An error occurred

Severity error

L2TPD_EVLIB_TIMER_SET_FAILED

System Log Message Unable to set event timer: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not set an event timer for the indicated reason.

Type Error: An error occurred

Severity error

L2TPD_FILTER_FILE_OPEN_FAILED

System Log Message Unable to open file *filename*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not open the indicated filter file.

Type Error: An error occurred

Severity error

L2TPD_GLOBAL_CFG_ADD_FAILED

System Log Message Unable to add global configuration for PIC *pic-slot* (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add the global configuration for the indicated Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_GLOBAL_CFG_CHANGE_FAILED

System Log Message Unable to change global configuration for PIC *pic-slot* (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not change the global configuration for the indicated Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_GLOBAL_CFG_DELETE_FAILED

System Log Message Unable to delete global configuration for PIC *pic-slot* (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete the global configuration for the indicated Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_IFD_ADD_FAILED

System Log Message *function-name*: unable to add interface device *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add the indicated interface device to the in-memory database.

Type Error: An error occurred

Severity error

L2TPD_IFD_DELETE_FAILED

System Log Message *function-name*: unable to delete interface device *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not delete the indicated interface device from the in-memory database.

Type Error: An error occurred

Severity error

L2TPD_IFD_MSG_REGISTER_FAILED

System Log Message Unable to register message handler for interface device: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not register an interface device message handler.

Type Error: An error occurred

Severity error

L2TPD_IFD_ROOT_ALLOC_FAILED

System Log Message Unable to allocate memory for interface device root node: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not allocate memory in the in-memory database for the root node for an interface device.

Type Error: An error occurred

Severity error

L2TPD_IFL_ADD_FAILED

System Log Message *function-name*: unable to add interface *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add the indicated logical interface to the in-memory database.

Type Error: An error occurred

Severity error

L2TPD_IFL_DELETE_FAILED

System Log Message *function-name*: unable to delete interface *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not delete the indicated logical interface from the in-memory database.

Type Error: An error occurred

Severity error

L2TPD_IFL_MSG_REGISTER_FAILED

System Log Message Unable to register message handler for interface: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not register a logical interface message handler.

Type Error: An error occurred

Severity error

L2TPD_IFL_NOT_FOUND

System Log Message Unable to find logical interface (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not retrieve a logical interface in the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_IFL_ROOT_ALLOC_FAILED

System Log Message Unable to allocate memory for interface root node: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not allocate memory in the in-memory database for the root node for a logical interface.

Type Error: An error occurred

Severity error

L2TPD_INSTANCE_CREATE_FAILED

System Log Message Unable to create L2TP instance *tunnel-group*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create an L2TP instance for the indicated tunnel group.

Type Error: An error occurred

Severity error

L2TPD_INSTANCE_RESTART_FAILED

System Log Message Unable to trigger restart of L2TP instance *tunnel-group*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not restart the L2TP instance for the indicated tunnel group.

Type Error: An error occurred

Severity error

L2TPD_INTERFACE_ID_NOT_FOUND

System Log Message Unable to find interface ID *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not find the indicated interface ID in the copy of the JUNOS configuration database that it maintains in memory.

Type Error: An error occurred

Severity error

L2TPD_MESSAGE_REGISTER_FAILED

System Log Message Unable to register L2TP message handler: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not register an L2TP message handler.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_BUNDLE_ALLOC_FAILED

System Log Message Unable to allocate MLPPP bundle

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate memory for a multilink Point-to-Point Protocol (MLPPP) bundle.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_BUNDLE_CREATE_FAILED

System Log Message Unable to create MLPPP bundle (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create a multilink Point-to-Point Protocol (MLPPP) bundle in the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_BUNDLE_INVALID_ID

System Log Message MLPPP bundle ID was invalid

Description The identifier assigned to a multilink Point-to-Point Protocol (MLPPP) bundle was invalid.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_COPY_CFG_FAILED

System Log Message Unable to copy MLPPP configuration (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not copy the multilink Point-to-Point Protocol (MLPPP) configuration for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_ID_ALLOC_FAILED

System Log Message Unable to allocate MLPPP ID map

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate memory for a multilink Point-to-Point Protocol (MLPPP) identifier map data structure.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_ID_BITMAP_ALLOC_FAIL

System Log Message Unable to allocate bitmap field for MLPPP ID map

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate memory for a bitmap field in a multilink Point-to-Point Protocol (MLPPP) identifier map data structure.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_ID_NODE_ADD_FAILED

System Log Message Unable to add node for bundle *bundle* to MLPPP ID map

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a node for the indicated multilink Point-to-Point Protocol (MLPPP) bundle to an MLPPP identifier map data structure.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_ID_ROOT_ALLOC_FAILED

System Log Message Unable to allocate root node for MLPPP ID map

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate the root note for a multilink Point-to-Point Protocol (MLPPP) identifier map data structure.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_LINK_CREATE_FAILED

System Log Message Unable to create MLPPP bundle links (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create multilink Point-to-Point Protocol (MLPPP) bundle links for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_LINK_MAX_EXCEEDED

System Log Message Unable to add link: maximum number of sessions exceeded for MLPPP bundle *bundle* (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a link for the indicated multilink Point-to-Point Protocol (MLPPP) bundle in the indicated tunnel and session, because the maximum number of links was exceeded.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_POOL_ADDRESS_FAILED

System Log Message Unable to assign pool address for MLPPP bundle *bundle* (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not assign a pool address for the indicated multilink Point-to-Point Protocol (MLPPP) bundle in the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_SESSION_CREATE_FAIL

System Log Message Unable to create MLPPP session (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create a multilink Point-to-Point Protocol (MLPPP) session for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_SESSION_DELETE_FAIL

System Log Message Unable to delete session for MLPPP bundle *bundle* (L2TP tunnel *tunnel-id*, session *session-id*, errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete the session configuration for the indicated multilink Point-to-Point Protocol (MLPPP) bundle in the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_MLPPP_SPEED_MISMATCH

System Log Message Unable to add link: speed differs for bundle *bundle* (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a link for the indicated multilink Point-to-Point Protocol (MLPPP) bundle in the indicated tunnel and session, because the bundle speed does not match.

Type Error: An error occurred

Severity error

L2TPD_NH_DELETE_FAILED

System Log Message Unable to delete next hop *next-hop*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete the indicated next hop.

Type Error: An error occurred

Severity error

L2TPD_POLICER_ADD_FAILED

System Log Message Unable to add policer *filter-name* (L2TP tunnel *tunnel-id*, session *session-id*): *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add the indicated policer to the indicated session on the indicated tunnel, which is associated with a user.

Type Error: An error occurred

Severity error

Action Remove the policer from the RADIUS database or contact your technical support representative.

L2TPD_POLICER_PROFILE_DEL_FAILED

System Log Message Unable to delete policer profile (L2TP tunnel *tunnel-id*, session *session-id*): *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete a policer profile from the indicated session on the indicated tunnel, which is associated with a user.

Type Error: An error occurred

Severity error

Action Remove the policer profile from the RADIUS database or contact your technical support representative.

L2TPD_POOL_ADDRESS_FAILED

System Log Message Unable to assign pool address (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not assign a pool address in the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_POOL_ASSIGN_ADDRESS_FAILED

System Log Message Unable to assign L2TP pool address: pool *pool-name* is invalid or has no free addresses

Description The Layer 2 Tunneling Protocol process (l2tpd) could not assign an address from the indicated address pool, either because the pool was invalid or had no free addresses.

Type Error: An error occurred

Severity error

L2TPD_PPP_ROUTE_ADD_FAILED

System Log Message Unable to add PPP peer route (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add information about a Point-to-Point Protocol (PPP) peer route to the in-memory configuration for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_PPP_ROUTE_DELETE_FAILED

System Log Message Unable to remove PPP peer route (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not delete information about a Point-to-Point Protocol (PPP) peer route from the in-memory configuration for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_PROFILE_NOT_FOUND

System Log Message Profile *profile-name* not found

Description The Layer 2 Tunneling Protocol process (l2tpd) could not locate an access profile from the configuration in order to find radius servers to authenticate.

Type Error: An error occurred

Severity error

L2TPD_PROFILE_NO_RADIUS_SERVERS

System Log Message Can't find radius servers for profile '*profile-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not locate any radius servers for the configured access profile.

Type Error: An error occurred

Severity error

L2TPD_RADIUS_ACCT_PORT_ZERO

System Log Message RADIUS server accounting port is zero

Description The Layer 2 Tunneling Protocol process (l2tpd) determined that the RADIUS server accounting port is zero, which is not a valid value.

Type Error: An error occurred

Severity error

L2TPD_RADIUS_GETHOSTNAME_FAILED

System Log Message Unable to obtain hostname for outgoing RADIUS message: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not obtain a hostname for an outgoing RADIUS message.

Type Error: An error occurred

Severity error

L2TPD_RADIUS_RT_INST_ENOENT

System Log Message Ignoring RADIUS server *radius-server*: routing instance *routing-instance* did not exist

Description The Layer 2 Tunneling Protocol process (l2tpd) did not use the indicated RADIUS server because the indicated routing instance specified for the server did not exist.

Type Error: An error occurred

Severity notice

L2TPD_RADIUS_RT_INST_NOT_FOUND

System Log Message Ignoring RADIUS server *radius-server*: unable to retrieve routing instance *routing-instance* (*error-message*)

Description The Layer 2 Tunneling Protocol process (l2tpd) did not use the indicated RADIUS server because it could not retrieve the indicated routing instance specified for the server.

Type Error: An error occurred

Severity error

L2TPD_RADIUS_SERVER_NOT_FOUND

System Log Message Unable to find RADIUS server (tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not locate a RADIUS server during Point-to-Point Protocol (PPP) authentication of the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_RADIUS_SRC_ADDR_BIND_FAIL

System Log Message Ignoring RADIUS server *radius-server*: unable to bind to source address *source-address* (*error-message*)

Description The Layer 2 Tunneling Protocol process (l2tpd) did not use the indicated RADIUS server because it could not bind to the indicated source address.

Type Error: An error occurred

Severity error

L2TPD_RADIUS_SRC_ADDR_ENOENT

System Log Message Ignoring RADIUS server *radius-server*: source address *source-address* did not exist

Description The Layer 2 Tunneling Protocol process (l2tpd) did not use the indicated RADIUS server because the indicated source address did not exist in the routing instance for the server.

Type Error: An error occurred

Severity notice

L2TPD_RPD_ASYNC_UNREG_FAILED

System Log Message Unable to unregister with rpd (*return-value*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not unregister asynchronously with the routing protocol process (rpd).

Type Error: An error occurred

Severity error

L2TPD_RPD_ROUTE_ADD_CB_FAILED

System Log Message Unable to add route *address/prefix-length* asynchronously (gateway *gateway-id* [*gateway-name*], L2TP tunnel *tunnel-id*, session *session-id*): *error-code*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a route on an asynchronous callback for the indicated address and prefix, gateway, tunnel, and session.

Type Error: An error occurred

Severity error

L2TPD_RPD_ROUTE_ADD_FAILED

System Log Message Unable to add route *address/prefix-length* (gateway *gateway-id* [*gateway-name*], L2TP tunnel *tunnel-id*, session *session-id*): *error-message* (*error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a route for the indicated address and prefix, gateway, tunnel, and session.

Type Error: An error occurred

Severity error

L2TPD_RPD_ROUTE_DELETE_CB_FAILED

System Log Message Unable to delete route *address/prefix-length* asynchronously (gateway *gateway-id* [*gateway-name*], L2TP tunnel *tunnel-id*, session *session-id*): *error-code*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete a route on an asynchronous callback for the indicated address and prefix, gateway, tunnel, and session.

Type Error: An error occurred

Severity error

L2TPD_RPD_ROUTE_DELETE_FAILED

System Log Message Unable to delete route *address/prefix-length* (gateway *gateway-id* [*gateway-name*], L2TP tunnel *tunnel-id*, session *session-id*): *error-message* (*error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete a route for the indicated address and prefix, gateway, tunnel, and session.

Type Error: An error occurred

Severity error

L2TPD_RPD_ROUTE_PREFIX_TOO_LONG

System Log Message Unable to add route *address/prefix-length*: prefix too long (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a route for the indicated address and prefix, tunnel, and session.

Type Error: An error occurred

Severity error

L2TPD_RPD_SESS_CREATE_FAILED

System Log Message Unable to establish session with rpd (*error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not establish a session with the routing protocol process (rpd).

Type Error: An error occurred

Severity error

L2TPD_RPD_SESS_HANDLE_ALLOC_FAIL

System Log Message Unable to allocate session handle for rpd connection: *error-message* (*error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate a session handle while attempting to initialize a connection to the routing protocol process (rpd).

Type Error: An error occurred

Severity error

L2TPD_RPD_SOCKET_ALLOC_FAILED

System Log Message Unable to allocate socket address for rpd connection

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate a socket address structure while attempting to initialize a connection to the routing protocol process (rpd).

Type Error: An error occurred

Severity error

L2TPD_RPD_TBL_LOCATE_BY_NAME

System Log Message Unable to locate rpd table by name: *error-message* (*error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) attempted to retrieve a routing protocol process table by providing the table name. The attempt failed.

Type Error: An error occurred

Severity error

L2TPD_RPD_TBL_LOCATE_FAILED

System Log Message Unable to locate table *table-name* for *identifier* (*return-value*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not retrieve the indicated routing protocol process table.

Type Error: An error occurred

Severity error

L2TPD_RPD_VERSION_MISMATCH

System Log Message Versions of rpd and librpd did not match; not retrying

Description The Layer 2 Tunneling Protocol process (l2tpd) determined that the versions of the routing protocol process (rpd) and routing protocol library (librpd) were different. It halted its attempt to connect to the rpd process.

Type Error: An error occurred

Severity error

L2TPD_RTSLIB_ASYNC_OPEN_FAILED

System Log Message Unable to open asynchronous routing socket connection

Description The Layer 2 Tunneling Protocol process (l2tpd) could not open a routing socket connection asynchronously. It uses the connection to communicate with the JUNOS operating system kernel.

Type Error: An error occurred

Severity error

L2TPD_RTSLIB_OPEN_FAILED

System Log Message Unable to open routing socket connection

Description The Layer 2 Tunneling Protocol process (l2tpd) could not open a routing socket connection, which it uses to communicate with the JUNOS operating system kernel.

Type Error: An error occurred

Severity error

L2TPD_SERVER_START_FAILED

System Log Message Startup of L2TP server failed

Description The Layer 2 Tunneling Protocol (L2TP) server did not start.

Type Error: An error occurred

Severity error

L2TPD_SERVICE_NH_ADD_FAILED

System Log Message Unable to add service next hop (L2TP tunnel *tunnel-id*, session *session-id*): *error-message* (*error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add information about a service next hop to the in-memory configuration for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SERVICE_NH_DELETE_FAILED

System Log Message Unable to remove service next hop *next-hop* (VRF *vrf*, L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not remove information about the indicated service next hop from the in-memory configuration for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_CFG_ADD_ERROR

System Log Message Unable to add L2TP tunnel *tunnel-id*, session *session-id* to PIC configuration (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add information about the indicated session and tunnel to the in-memory configuration for the Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_SESSION_CFG_ADD_FAILED

System Log Message Unable to add L2TP tunnel *tunnel-id*, session *session-id* to PIC configuration

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add information about the indicated session and tunnel to the in-memory configuration for the Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_SESSION_CFG_DELETE_FAILED

System Log Message Unable to remove L2TP tunnel *tunnel-id*, session *session-id* from PIC configuration

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not remove information about the indicated session and tunnel from the in-memory configuration for the Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_SESSION_DELETE_FAILED

System Log Message Unable to delete session (L2TP tunnel *tunnel-id*, session *session-id*, errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete information about the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFF_NOT_FOUND

System Log Message Unable to find family structure for interface *interface-name* (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not retrieve the interface family structure for the indicated logical interface index in the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_ADD_FAILED

System Log Message *function-name*: unable to assign session *session-id* to interface *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not associate the indicated session with the indicated logical interface.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_ALLOC_FAILED

System Log Message *function-name*: unable to allocate memory for session *session-id*, interface *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate memory for the indicated session to be associated with the indicated logical interface.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_CLI_TREE_ALLOC

System Log Message Unable to allocate memory for session tree for interface *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not allocate memory for a command-line interface (CLI)-specific session tree structure for the indicated logical interface.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_DELETED

System Log Message *function-name*: interface *interface-name* is deleted

Description The Layer 2 Tunneling Protocol process (l2tpd) detected that the configuration information for the indicated logical interface was deleted for a session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_DELETE_FAILED

System Log Message *function-name*: unable to delete session *identifier* from interface *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete information about a session from the configuration information for a logical interface.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_GET_FAILED

System Log Message *function-name*: unable to find interface *interface-name*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not retrieve configuration information about the indicated logical interface, to which it was going to add session information.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_NOT_EQUAL

System Log Message *function-name*: interface *interface-name* not equal

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a session for the indicated logical interface.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_NOT_FOUND

System Log Message Unable to find interface *interface-name* (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not find the indicated logical interface corresponding to the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_OCCUPIED

System Log Message *function-name*: interface *interface-name* already has associated session (*value1*/*value2*)

Description The Layer 2 Tunneling Protocol process (l2tpd) determined that the indicated logical interface already had an associated session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_IFL_REMOVE_FAILED

System Log Message Unable to remove L2TP tunnel *tunnel-id*, session *session-id* from logical interface (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not remove information about the indicated tunnel and session from the record it maintains for a logical interface.

Type Error: An error occurred

Severity error

L2TPD_SESSION_INVALID_PEER_IP

System Log Message Invalid peer address *peer-address* in IPCP UP (L2TP tunnel *tunnel-id*, session *session-id*); closing session

Description The Layer 2 Tunneling Protocol process (l2tpd) received an IP Control Protocol (IPCP) 'UP' message for the indicated tunnel and session that included the indicated IP address for a peer. The address was invalid, and the l2tpd process started closing down the session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_ROUTE_ADD_FAILED

System Log Message Unable to add PPP route (L2TP tunnel *tunnel-id*, session *session-id*, errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not add a Point-to-Point Protocol (PPP) route for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_RT_TBL_NOT_FOUND

System Log Message Unable to find route table *table-id* for interface *interface-name* (L2TP tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not retrieve the indicated routing table associated with the indicated logical interface in the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SESSION_TUNNEL_ID_MISMATCH

System Log Message Tunnel ID *tunnel-id* in message does not match L2TP tunnel *l2tp-tunnel-id*, session *session-id*

Description The Layer 2 Tunneling Protocol process (l2tpd) received a message with the indicated tunnel identifier, which did not match the identifier stored for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_SETSOCKOPT_FAILED

System Log Message setsockopt() failed *operation*: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not set socket options during the indicated operation.

Type Error: An error occurred

Severity error

L2TPD_SET_ASYNC_CONTEXT

System Log Message Unable to set asynchronous context (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not set asynchronous context for a routing socket connection, which it uses to communicate with the JUNOS operating system kernel.

Type Error: An error occurred

Severity error

L2TPD_SHOW_MULTILINK

System Log Message Detail level *level* is not supported by 'show services l2tp multilink' command

Description The 'show services l2tp multilink' command was issued with the indicated option to specify the amount of information to return, but the command does not support that option.

Type Error: An error occurred

Severity error

L2TPD_SHOW_SESSION

System Log Message Detail level *level* is not supported by 'show services l2tp session' command

Description The 'show services l2tp session' command was issued with the indicated option to specify the amount of information to return, but the command does not support that option.

Type Error: An error occurred

Severity error

L2TPD_SHOW_TUNNEL

System Log Message Detail level *level* is not supported by 'show services l2tp tunnel' command

Description The 'show services l2tp tunnel' command was issued with the indicated option to specify the amount of information to return, but the command does not support that option.

Type Error: An error occurred

Severity error

L2TPD_SOCKET_FAILED

System Log Message socket() failed *operation*: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not open socket during the indicated operation.

Type Error: An error occurred

Severity error

L2TPD_SUBUNIT_ROUTE_ALLOC_FAILED

System Log Message Unable to allocate L2TP route (tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not allocate a subunit route record for the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_TRACE_FILE_OPEN_FAILED

System Log Message Unable to open trace file: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not open its trace file.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_CFG_ADD_FAILED

System Log Message Unable to add L2TP tunnel *tunnel-id* to PIC configuration (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add information about the indicated tunnel to the in-memory configuration for the Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_CFG_ADD_INV_ADDR

System Log Message Unable to add L2TP tunnel *tunnel-id* to PIC configuration: address invalid

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add information about the indicated tunnel to the in-memory configuration for the Physical Interface Card (PIC), because the local or remote address provided for the tunnel was invalid.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_CFG_DELETE_FAILED

System Log Message Unable to remove L2TP tunnel *tunnel-id* from PIC configuration

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not remove information about the indicated tunnel from the in-memory configuration for the Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_DELETE_FAILED

System Log Message Unable to delete L2TP tunnel *tunnel-id* (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete information about the indicated tunnel.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_DEST_IF_LOOKUP_FAIL

System Log Message Unable to find destination interface for L2TP tunnel *tunnel-id* remote address: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) tried to use route lookup to determine which local logical interface to use to reach the remote end of the indicated tunnel. The attempt failed.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_GROUP_ADD_FAILED

System Log Message Unable to create L2TP tunnel group

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create a tunnel group.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_GROUP_CFG_ADD_FAIL

System Log Message Unable to add tunnel group *tunnel-group* (service set *service-set*) to configuration for PIC *pic-slot*: *error-message*

Description The Layer 2 Tunneling Protocol process (l2tpd) maintains a copy of the JUNOS configuration database in memory. It could not add information about the indicated tunnel group and service set to the in-memory configuration for the indicated Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_GROUP_CFG_DEL_FAIL

System Log Message Unable to delete tunnel group *tunnel-group* (service set *service-set*): *error-code*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete information about the indicated tunnel group and service set.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_GROUP_CREATE_FAILED

System Log Message Unable to create L2TP module for tunnel group *address*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not create the indicated protocol tunnel group.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_GROUP_DELETE_FAILED

System Log Message Unable to delete L2TP tunnel group *tunnel-group-id* (errno *error-code*)

Description The Layer 2 Tunneling Protocol process (l2tpd) could not delete information about the indicated tunnel group.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_GROUP_IDX_MISMATCH

System Log Message Tunnel group index *index1* in message does not match index *index2* stored for L2TP tunnel *tunnel-id*

Description The Layer 2 Tunneling Protocol process (l2tpd) received a message with the indicated tunnel group index, which did not match the indicated group tunnel index stored for the indicated tunnel.

Type Error: An error occurred

Severity error

L2TPD_TUNNEL_GROUP_RESTART_FAIL

System Log Message Unable to restart L2TP module for tunnel group

Description The Layer 2 Tunneling Protocol process (l2tpd) could not restart a protocol tunnel group.

Type Error: An error occurred

Severity error

L2TPD_USER_AUTHN_NOT_FOUND

System Log Message Unable to find user profile *username* during PPP authentication

Description The Layer 2 Tunneling Protocol process (l2tpd) could not retrieve the user profile for the indicated username, which it needs for Point-to-Point Protocol (PPP) authentication of a session.

Type Error: An error occurred

Severity error

L2TPD_USER_AUTHN_ORDER_UNKNOWN

System Log Message Unknown authentication order *authentication-order* (tunnel *tunnel-id*, session *session-id*)

Description The Layer 2 Tunneling Protocol process (l2tpd) did not recognize the indicated authentication order, which was specified for Point-to-Point (PPP) authentication of the indicated tunnel and session.

Type Error: An error occurred

Severity error

L2TPD_USER_AUTHN_PWD_NOT_FOUND

System Log Message Unable to retrieve password during PPP authentication of user *username*

Description The Layer 2 Tunneling Protocol process (l2tpd) could not retrieve the password for the indicated username, which it needs for Point-to-Point Protocol (PPP) authentication of a session.

Type Error: An error occurred

Severity error

Chapter 37

LACPD System Log Messages

This chapter describes messages with the LACPD prefix. They are generated by the Link Aggregation Control Protocol (LACPD) process (lacpd), which supports LACP functions for aggregated Ethernet interfaces.

LACPD_MEMORY_ALLOCATION_FAILED

System Log Message Unable to allocate memory for interface *interface-name*

Description The Link Aggregation Control Protocol process (lacpd) could not allocate memory for the indicated interface.

Type Error: An error occurred

Severity error

Chapter 38

LFMD System Log Messages

This chapter describes messages with the LFMD prefix. They are generated by the link-fault management process (lfmd), which supports Operation, Administration, and Maintenance (OAM) functions that are defined in the Institute of Electrical and Electronics Engineers (IEEE) 802.3ah standard for Ethernet interfaces.

LFMD_RTSOCK_OPEN_FAILED

System Log Message Unable to open synchronous routing socket: *error-message*

Description The Ethernet Operation, Administration and Management link-fault management process (lfmd) could not open a routing socket to create a connection.

Type Error: An error occurred

Severity error

Chapter 39

LIBESPTASK System Log Messages

This chapter describes messages with the LIBESPTASK prefix.

LIBESPTASK_SNMP_CONN_PROG

System Log Message *function-name*: *error-message*

Description The indicated error occurred while the process using libesptask was connecting to the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity info

LIBESPTASK_SNMP_CONN_QUIT

System Log Message *function-name*: unable to connect to SNMP agent (*pathname*): *error-message*

Description The process using libesptask could not connect to the indicated Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

LIBESPTASK_SNMP_CONN_RETRY

System Log Message *function-name*: reattempting connection to SNMP agent (*pathname*): *error-message*

Description The process using libesptask tried again to connect to the indicated Simple Network Management Protocol (SNMP) master agent after a connection attempt failed.

Type Error: An error occurred

Severity error

LIBESPTASK_SNMP_INVALID_SOCKET

System Log Message *function-name*: socket *file-descriptor* is invalid

Description The process using libesptask could not send a message to a Simple Network Management Protocol (SNMP) master agent because the indicated socket is invalid.

Type Error: An error occurred

Severity error

LIBESPTASK_SNMP_SOCKOPT_BLOCK

System Log Message *function-name*: unable to set nonblocking option

Description The process using libesptask could not set a socket to nonblocking mode after connecting to the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

LIBESPTASK_SNMP_SOCKOPT_RECVBUF

System Log Message *function-name*: unable to set recvbuf option

Description The process using libesptask could not set the size of the kernel receive buffer, which allows it to accept the largest possible packet from the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

LIBESPTASK_SNMP_SOCKOPT_SENDBUF

System Log Message *function-name*: unable to set sendbf option

Description The process using libesptask could not set the size of the kernel send buffer, which allows it to send the largest possible packet to the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

Chapter 40

LIBJNX System Log Messages

This chapter describes messages with the LIBJNX prefix. They are generated by processes that call routines in the libjuniper library, which includes routines for creating and managing child processes, parsing machine and interface addresses, tracing, file I/O, and other functions.

LIBJNX_AUDIT_ERROR

System Log Message *function-name*: *error-message*

Description A JUNOS process could not notify the audit process (auditd) about user activity related to system accounting, because of an interprocess communication (IPC) error.

Type Error: An error occurred

Severity error

Cause Possible reasons include (a) auditd was not running (b) auditd was still initializing after a restart (c) there was a socket error.

Action Contact your technical support representative.

LIBJNX_COMPRESS_EXEC_FAILED

System Log Message Unable to compress file '*filename*' using *program-name*: *error-message*

Description A JUNOS process tried to use the indicated utility to create a compressed version of the indicated old system log file. The attempt failed for the indicated reason.

Type Error: An error occurred

Severity info

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_DEFAULT_IP_ADDR_NOT_SET

System Log Message Unable to retrieve system default IP address: not set in kernel (*error-message*)

Description A JUNOS process could not retrieve the system default IP address from the kernel, because the address is not defined there.

Type Error: An error occurred

Severity critical

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_EVLIB_FAILURE

System Log Message *function-name*: *error-message*

Description A JUNOS process called the indicated function in the event library. The function failed for the indicated reason.

Type Error: An error occurred

Severity emergency

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_EXEC_EXITED

System Log Message Command stopped: PID *pid*, signal = '*return-value*'*core-dump-status*, command '*command*'

Description A JUNOS process created a child process to execute the indicated command for it. The child process stopped unexpectedly.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_EXEC_FAILED

System Log Message Child exec failed for command '*command*': *error-message*

Description A JUNOS process called the exec() system call while creating a child process to execute the indicated command for it. The system call failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_EXEC_PIPE

System Log Message Unable to create pipes for command '*command*': *error-message*

Description A JUNOS process created a child process to execute the indicated command for it. Its attempt to create pipes for communication with the child failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_EXEC_SIGNALED

System Log Message Command received signal: PID *pid*, signal *signal-namecore-dump-status*, command '*command*'

Description A JUNOS process created a child process to execute the indicated command for it. The child process received the indicated signal and exited.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_EXEC_WEXIT

System Log Message Command exited: PID *pid*, status *return-valuecore-dump-status*, command '*command*'

Description A JUNOS process created a child process to execute the indicated command for it. The child process exited abnormally with the indicated exit code.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_FILE_COPY_FAILED

System Log Message Failed to copy from *source-filename* to *destination-filename*

Description A JUNOS process could not copy the indicated source file to the indicated destination name or location.

Type Error: An error occurred

Severity error

LIBJNX_FILE_SYSTEM_FAIL

System Log Message *pathname*: *error-message*

Description A JUNOS process could not obtain status information for the indicated file system.

Type Event: This message reports an event, not an error

Severity error

LIBJNX_FILE_SYSTEM_SPACE

System Log Message Not enough space left on device *pathname*

Description A JUNOS process found that the indicated file system did not have the free space needed for storing temporary files.

Type Event: This message reports an event, not an error

Severity warning

LIBJNX_INVALID_CHASSIS_ID

System Log Message *function-name*: invalid chassis ID *chassis-id*

Description A JUNOS process could not determine the hostname for the master Routing Engine on a routing node in a routing matrix, because the indicated chassis ID provided for the routing platform was invalid.

Type Error: An error occurred

Severity error

LIBJNX_INVALID_RE_SLOT_ID

System Log Message *function-name*: invalid Routing Engine slot ID *routing-engine-slot*

Description A JUNOS process could not determine the hostname for a Routing Engine, because the indicated Routing Engine slot ID was invalid.

Type Error: An error occurred

Severity error

LIBJNX_INVALID_XML_DATA

System Log Message Invalid XML data '*data*'

Description The XML parser closed its session with a client application because the indicated XML data sent by the client was invalid.

Type Error: An error occurred

Severity error

LIBJNX_PRIV_LOWER_FAILED

System Log Message Unable to lower privilege level: *error-message*

Description A JUNOS process attempted to revert its effective user ID to the original user. The attempt failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_PRIV_RAISE_FAILED

System Log Message Unable to raise privilege level: *error-message*

Description A JUNOS process attempted to set its effective user ID to the root user. The attempt failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_REPLICATE_RCP_ERROR

System Log Message *operation*: *operational-status*

Description The rcp command failed during replication.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_REPLICATE_RCP_EXEC_FAILED

System Log Message rcp failed: *error-message*

Description A JUNOS process created a child process to copy a file to the other Routing Engine. The copy operation failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_SNMP_ENGINE_FILE_FAILURE

System Log Message *function-name*: operation: *operation filename*: *error-message*

Description A JUNOS process could not perform the indicated operation on the indicated SNMP engine data file.

Type Error: An error occurred

Severity critical

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_SOCKET_FAILURE

System Log Message *operation*: *error-message*

Description Various system processes use Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Reliable Data Protocol (RDP) sockets. The indicated socket operation failed for the indicated reason.

Type Error: An error occurred

Severity emergency

Cause An internal software failure occurred.

Action Contact your technical support representative.

LIBJNX_XML_DECODE_FAILED

System Log Message Invalid XML encoding '*data*', skipping to ';'

Description The XML parser ignored the indicated XML data sent by a client application, because the XML encoding of the data was invalid. The parser skipped ahead to the likely endpoint for the invalid data.

Type Error: An error occurred

Severity error

Cause A possible cause is improper escaping of character constants in the data stream.

Action Contact your technical support representative.

Chapter 41

LIBMSPRPC System Log Messages

This chapter describes messages with the LIBMSPRPC prefix. They are generated by the mspinfo process, which is responsible for RPC communication between the Routing Engine (RE) and the Multiservcies Physical Interface Cards (PICs).

LIBMSPRPC_CLIENT_INIT_FAILED

System Log Message Can't create msprpc client: *error-message*

Description A JUNOS process (mspinfo) could not establish initialization of the RPC client.

Type Error: An error occurred

Severity error

Cause Possible reasons: process is out of memory

Action Contact your technical support representative.

LIBMSPRPC_CLIENT_KCOM_FAILED

System Log Message Can't initialize kcom for msprpc client: *error-message*

Description A JUNOS process (mspinfo) could not establish initialization of the kcom subsystem.

Type Error: An error occurred

Severity error

Cause Possible reasons: can't initialize kcom services.

Action Contact your technical support representative.

LIBMSPRPC_CLIENT_NO_CONNECTION

System Log Message Failed connecting fpc = *fpc-slot*, pic = *pic-slot*

Description Remote execution of the command given from the RE to the PIC failed, can not connect to the PIC.

Type Error: An error occurred

Severity notice

Cause Possible reasons: a)PIC appears online but is not responding b)msprpc server is not running on the PIC.

Action Contact your technical support representative.

LIBMSPRPC_CLIENT_NO_REPLY

System Log Message Error executing "*command*": no reply from the PIC

Description Remote execution of the command given from the RE to the PIC failed, no reply from the PIC.

Type Error: An error occurred

Severity notice

Cause Possible reasons: a)wrong command b)insufficient permissions c)wrong arguments d)PIC appears online but is not responding e)msprpc server is not running on the PIC.

Action Contact your technical support representative.

LIBMSPRPC_CLIENT_PIC_DOWN

System Log Message Interface *interface-name* is down

Description Remote execution of the command given from the RE to the PIC failed, the PIC is down.

Type Error: An error occurred

Severity error

Cause Possible reasons: the given PIC is not responding and/or is offline.

Action Contact your technical support representative.

LIBMSPRPC_CLIENT_WRONG_OUTPUT

System Log Message Error executing "*command*": output length exceeds *correct-length* characters

Description Remote execution of the command given from the RE to the PIC failed, PIC returned unexpected output.

Type Error: An error occurred

Severity notice

Cause Possible reasons: a)wrong command b)wrong arguments.

Action Contact your technical support representative.

Chapter 42

LICENSE System Log Messages

This chapter describes messages with the LICENSE prefix. They are generated by processes that call routines in the liblicense library, which provide software license management functions on a routing platform.

LICENSE_CONNECT_FAILURE

System Log Message Connection could not be set up: *error-message*

Description The indicated error occured because a connection to the license-check process was not established.

Type Error: An error occurred

Severity error

LICENSE_CONN_TO_LI_CHECK_FAILURE

System Log Message Process could not connect to license-check in *maximum-value* tries; giving up

Description The indicated process failed to connect to the license-check process after the indicated maximum tries.

Type Error: An error occurred

Severity error

LICENSE_CONN_TO_LI_CHECK_SUCCESS

System Log Message Connected to license-check

Description The indicated process succesfully connected to the license-check process.

Type Event: This message reports an event, not an error

Severity info

LICENSE_EXPIRED

System Log Message License for feature *feature-name*(*feature-id*) expired

Description The time-based license for the indicated feature expired. The feature remains inactive until a new license is installed.

Type Event: This message reports an event, not an error

Severity alert

LICENSE_GRACE_PERIOD_APPROACHING

System Log Message License grace period for feature *feature-name*(*feature-id*) will expire in *time*

Description The indicated amount of time remained before the license grace period for the indicated feature would expire. If a new license was not installed within that time, the feature became inactive.

Type Event: This message reports an event, not an error

Severity alert

LICENSE_GRACE_PERIOD_EXCEEDED

System Log Message License grace period for feature *feature-name*(*feature-id*) will expire in *time* (limit = *maximum-value*)

Description The grace period for a scale license is about to expire. Unless the scale license is upgraded, the license will scale back to the licensed limit once the grace period expires.

Type Event: This message reports an event, not an error

Severity alert

LICENSE_GRACE_PERIOD_EXPIRED

System Log Message License grace period for feature *feature-name*(*feature-id*) has expired

Description The grace period for a licensable feature has expired. Strict license enforcement will remain active until a new license is installed.

Type Event: This message reports an event, not an error

Severity alert

LICENSE_LIST_MANAGEMENT

System Log Message Error occurred for feature *feature-name*: *error-message* (system error: *system-error-message*)

Description The management process (mgd) could not complete a license management command related to the indicated feature. If a system error is reported, it caused the problem.

Type Error: An error occurred

Severity error

LICENSE_NEARING_EXPIRY

System Log Message License for feature *feature-name*(*feature-id*) expires in *time*

Description At the time this message was logged, the indicated amount of time remained before the time-based license for the indicated feature would expire. If a new license was not installed within that time, the feature became inactive.

Type Event: This message reports an event, not an error

Severity alert

LICENSE_READ_ERROR

System Log Message recvmsg() failed:*error-message*

Description The indicated process failed to read an event sent to it, for the indicated reason.

Type Error: An error occurred

Severity error

LICENSE_REG_ERROR

System Log Message Registration request failed: *current-value*

Description The license registration request failed. A request needs to be resent to the license-check process.

Type Error: An error occurred

Severity error

LICENSE_SIGNATURE_VERIFY_FAILED

System Log Message Signature verification failed: *error-message*

Description The management process (mgd) could not verify a license because the license's signature was invalid.

Type Error: An error occurred

Severity error

LICENSE_UNKNOWN_RESPONSE_TYPE

System Log Message unknown message type received: *current-value*

Description An unknown response type was received from the license-check process.

Type Error: An error occurred

Severity error

LICENSE_VERIFICATION_FILE_ERROR

System Log Message License verification failed for file '*error-message*': *filename* (system error: *system-error-message*)

Description The management process (mgd) could not verify the indicated license file because of the indicated internal file-handling error.

Type Error: An error occurred

Severity error

Chapter 43

LLDPD System Log Messages

This chapter describes messages with the LLDPD prefix. They are generated by the Link Layer Discovery Protocol (lldpd) process, which is responsible for discovering network devices and their capabilities.

LLDPD_SYSTEM

System Log Message *reason*: *error-message*

Description A system call made by the Link Layer Discovery Protocol process (LLDPD) failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request. LLDPD will recover.

Chapter 44

LPDFD System Log Messages

This chapter describes messages with the LPDFD prefix. They are generated by the local policy decision function process. A policy decision function is a component in the IP multimedia subsystem which controls traffic entering the packet-switched network by allocating or denying IP bearer resources.

LPDFD_DYN_PDB_OPEN_FAILED

System Log Message Failed to open profile database: *error-message*

Description The local policy decision function process (lpdfd) failed to open the profile database.

Type Error: An error occurred

Severity error

LPDFD_DYN_REGISTER_FAILED

System Log Message Dynamic config register failed: *error-message*

Description The local policy decision function process (lpdfd) failed to register with the dynamic configuration subsystem.

Type Error: An error occurred

Severity error

LPDFD_DYN_SDB_OPEN_FAILED

System Log Message Failed to open session database: *error-message*

Description The local policy decision function process (lpdfd) failed to open the session database.

Type Error: An error occurred

Severity error

LPDFD_PCONN_SERVER

System Log Message *argument*: Cannot retrieve peer info for session. Error: *error-message*

Description The local policy decision function process (lpdfd) pconn server failed to initialize

Type Error: An error occurred

Severity error

Chapter 45

LOGIN System Log Messages

This chapter describes messages with the LOGIN prefix. They are generated by the login process (login), which performs authentication for Telnet sessions.

LOGIN_ABORTED

System Log Message Client aborted login

Description A login attempt was cancelled, either by the remote user or in response to a signal.

Type Event: This message reports an event, not an error

Severity info

LOGIN_FAILED

System Log Message Login failed for user *username* from host *hostname*

Description A login attempt failed for the indicated username.

Type Event: This message reports an event, not an error

Severity notice

LOGIN_FAILED_SET_CONTEXT

System Log Message Failed to set context for user *username*

Description The login process (login) could not set login context properties for the indicated user and cancelled the authentication attempt.

Type Error: An error occurred

Severity error

LOGIN_FAILED_SET_LOGIN

System Log Message Failed to set login ID for user *username*: *error-message*

Description The login process (login) could not assume the user ID of the indicated user and cancelled the authentication attempt.

Type Error: An error occurred

Severity error

LOGIN_HOSTNAME_UNRESOLVED

System Log Message Unable to resolve hostname *hostname*: *error-message*

Description The login process (login) could not resolve the indicated remote hostname for the indicated reason.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

LOGIN_INFORMATION

System Log Message User *username* logged in from host *hostname* on device *tty-name*

Description The indicated username was authenticated and logged into the shell specified for it in the password file.

Type Event: This message reports an event, not an error

Severity info

LOGIN_LOCAL_PASSWORD

System Log Message Requested local password from user *username*

Description The PAM authentication attempt failed for the indicated user, who was prompted for the password recorded in the local password file.

Type Event: This message reports an event, not an error

Severity info

LOGIN_MALFORMED_USER

System Log Message Invalid username: *username*

Description The indicated username was invalid.

Type Event: This message reports an event, not an error

Severity info

LOGIN_PAM_AUTHENTICATION_ERROR

System Log Message PAM authentication error for user *username*

Description The login process (login) could not authenticate the indicated user via PAM.

Type Event: This message reports an event, not an error

Severity error

LOGIN_PAM_ERROR

System Log Message Failure while authenticating user *username*: *error-message*

Description The PAM authentication process failed for the indicated username, for the indicated reason.

Type Error: An error occurred

Severity error

LOGIN_PAM_MAX_RETRIES

System Log Message Too many retries while authenticating user *username*

Description The number of failed PAM authentication attempts for the indicated user exceeded the maximum limit.

Type Error: An error occurred

Severity error

LOGIN_PAM_STOP

System Log Message Failed to end PAM session: *error-message*

Description The login process (login) could not end the PAM authentication session, for the indicated reason.

Type Error: An error occurred

Severity error

LOGIN_PAM_USER_UNKNOWN

System Log Message Attempt to authenticate unknown user *username*

Description The login process (login) failed to authenticate the indicated user via PAM because the username was unknown.

Type Event: This message reports an event, not an error

Severity error

LOGIN_PASSWORD_EXPIRED

System Log Message Forcing change of expired password for user *username*

Description The password provided for the indicated username was expired and the user was prompted to set a new one.

Type Event: This message reports an event, not an error

Severity info

LOGIN_REFUSED

System Log Message Login of user *username* from host *hostname* on device *tty-name* was refused: *reason*

Description A login attempt for the indicated username was rejected for the indicated reason.

Type Event: This message reports an event, not an error

Severity notice

LOGIN_ROOT

System Log Message User *username* logged in as root from host *hostname* on device *tty-name*

Description The indicated username was authenticated as a superuser and logged into the shell specified for the root user in the password file.

Type Event: This message reports an event, not an error

Severity info

LOGIN_TIMED_OUT

System Log Message Login attempt timed out after *duration* seconds

Description A login attempt failed to complete in the maximum time allowed.

Type Event: This message reports an event, not an error

Severity info

Chapter 46

LRMUX System Log Messages

This chapter describes messages with the LRMUX prefix. They are generated by the logical router multiplexer process (lrmuxd), which manages the multiple instances of the routing protocols process (rpd) on a machine running logical routers.

LRMUX_FAILED_EXEC

System Log Message Failed to exec *command*

Description The Logical Router Multiplexer process (lrmuxd) issued the exec() system call to start a routing process (rpd) to check the validity of the configuration. The system call failed.

Type Error: An error occurred

Severity error

LRMUX_LRPD_PID_LOCK

System Log Message Lock not found on PID file *filename*

Description The Logical Router Multiplexer process (lrmuxd) could not find a lock for a logical router.

Type Error: An error occurred

Severity error

Cause A logical router process (rpd) died.

LRMUX_LRPD_PID_OPEN

System Log Message Unable to open PID file *filename*

Description The Logical Router Multiplexer process (lrmuxd) could not open the indicated PID lock file for a logical router process (rpd).

Type Error: An error occurred

Severity error

LRMUX_LRPD_SEND_HUP

System Log Message Unable to send signal to PID *pid*

Description The Logical Router Multiplexer process (lrmuxd) could not forward a SIGHUP signal to a logical router process (rpd).

Type Error: An error occurred

Severity error

LRMUX_PID_LOCK

System Log Message Unable to lock PID file '*filename*'

Description The Logical Router Multiplexer process (lrmuxd) attempted to lock the file that records its process ID (PID), which serves to prevent multiple instances of the lrmuxd process from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

Chapter 47

MCSNOOPD System Log Messages

This chapter describes messages with the MCSNOOPD prefix. They are generated by the multicast snooping process (mcsnoopd), which enables a Layer 2 device to examine the content of Layer 3 packets to determine which actions to perform.

MCSNOOPD_MGMT_TIMEOUT

System Log Message Connection to management peer *process-name* timed out waiting for input

Description The connection between the snooping process (mcsnoopd) and the indicated management process (mgd) timed out before input arrived from the mgd process.

Type Error: An error occurred

Severity warning

Action Examine the messages that immediately follow this message in the system log for information about possible causes.

Cause An internal software failure occurred.

Chapter 48

MIB2D System Log Messages

This chapter describes messages with the MIB2D prefix. They are generated by the Management Information Base II (MIB II) process (mib2d), which services requests for information gathered and reported by the Simple Network Management Protocol (SNMP).

MIB2D_ATM_ERROR

System Log Message *function-name*: *error-message*

Description The MIB II process (mib2d) could not process ATM-related information.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_CONFIG_CHECK_FAILED

System Log Message *function-name*: configuration database has errors

Description The portion of the candidate configuration related to the MIB II process (mib2d) was checked for validity during a 'commit' operation. The check failed.

Type Error: An error occurred

Severity error

Cause The configuration was invalid.

Action Correct the invalid portion of the configuration as described in the error message on the console.

MIB2D_FILE_OPEN_FAILURE

System Log Message Unable to open file '*filename*': *error-message*

Description The MIB II process (mib2d) could not open the indicated file.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_IFD_IFDINDEX_FAILURE

System Log Message Ifd index assigned to *interface-name* changed from *old-value* to *new-value*, removing old interface

Description There was a change to the ifd Index assigned to the indicated existing interface.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_IFD_IFINDEX_FAILURE

System Log Message SNMP index assigned to *interface-name* changed from *old-value* to *new-value*

Description There was a change to the SNMP ifIndex assigned to the indicated existing interface.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_IFL_IFINDEX_FAILURE

System Log Message SNMP index assigned to *interface-name.interface-unit* changed from *old-value* to *new-value*

Description There was a change to the SNMP ifIndex assigned to the indicated existing interface.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_KVM_FAILURE

System Log Message *function-name*: *reason*: *error-message*

Description A call to the indicated function in the kernel virtual memory library failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_PMON_OVERLOAD_CLEARED_TRAP

System Log Message Overload name: *overload-name*, interface: *interface-name*

Description The MIB II process (mib2d) generated a jnxPMonOverloadCleared trap when it detected the clearing of an overload condition on the indicated monitoring services interface.

Type Event: This message reports an event, not an error

Severity warning

MIB2D_PMON_OVERLOAD_SET_TRAP

System Log Message Overload name: *overload-name*, interface: *interface-name*

Description The MIB II process (mib2d) generated a jnxPMonOverloadSet trap when it detected an overload condition on the indicated monitoring services interface.

Type Event: This message reports an event, not an error

Severity warning

MIB2D_RTSLIB_READ_FAILURE

System Log Message *function-name*: failed in *operation object-name*: *index* (*error-message*)

Description A call to the indicated function in the routing socket library failed during the indicated operation on the indicated object.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_RTSLIB_SEQ_MISMATCH

System Log Message *function-name*: sequence mismatch (*expected-value*, *received-value*), resyncing

Description The indicated function in the routing socket library detected a sequence number mismatch. The MIB II process (mib2d) will resynchronize its data with the JUNOS kernel.

Type Event: This message reports an event, not an error

Severity info

MIB2D_SNMP_INDEX_ASSIGN

System Log Message *function-name*: *reason* snmpid(*snmp-interface-index*) ifname(*interface-name.interface-unit*)

Description MIB2D can not assign snmp index for each interface.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_SNMP_INDEX_DUPLICATE

System Log Message *function-name*: duplicate snmpid(*snmp-interface-index*) old ifname(*interface-name.interface-unit*) new ifname(*new-interface-name.kernel-interface-unit*)

Description The SNMP index for first interface name was assigned the same SNMP index as second interface name.

Type Error: An error occurred

Severity emergency

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_SNMP_INDEX_UPDATE_STAT

System Log Message *function-name reason filename*

Description MIB2D can not get the status of SNMP index file

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_SNMP_INDEX_WRITE

System Log Message *function-name*: *reason filename*

Description MIB2D can not write into a file containing all the indices

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_SYSCTL_FAILURE

System Log Message *function-name*: sysctl *type* failed: *error-message*

Description A request to the JUNOS kernel for system data failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

MIB2D_TRAP_HEADER_FAILURE

System Log Message *function-name*: trap_request_header failed

Description The MIB II process (mib2d) could not allocate a trap header.

Type Error: An error occurred

Severity error

Cause The Routing Engine is low on memory.

Action Contact your technical support representative.

MIB2D_TRAP_SEND_FAILURE

System Log Message *function-name*: trap_request_send: *error-message*

Description The MIB II process (mib2d) could not send a trap header.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

Chapter 49

MPLS_OAM System Log Messages

This chapter describes messages with the MPLS_OAM prefix. They are generated by the Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) process (mplsoamd), which supports traceroute operations for LDP label-switched paths (LSPs).

MPLS_OAM_FANOUT_LIMIT_REACHED

System Log Message *fec-address*: traceroute fanout limit was reached

Description The traceroute fanout limit was reached.

Type Error: An error occurred

Severity info

Action Raise the traceroute fanout limit parameter.

MPLS_OAM_INVALID_SOURCE_ADDRESS

System Log Message *fec-address*: source address *ip-address* is invalid

Description The traceroute utility is configured to use an invalid source address.

Type Error: An error occurred

Severity error

Action Configure traceroute to use a valid source address.

MPLS_OAM_PATH_LIMIT_REACHED

System Log Message *fec-address*: traceroute path limit was reached

Description The traceroute path limit was reached.

Type Error: An error occurred

Severity info

Action Raise the traceroute path limit parameter.

MPLS_OAM_SEND_FAILED

System Log Message *fec-address*: unable to send probe (*error-message*)

Description The Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) process (mplsoamd) could not send a traceroute probe packet.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

MPLS_OAM_SOCKET_OPEN_FAILED

System Log Message *fec-address*: unable to open socket (*error-message*)

Description The Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) process (mplsoamd) could not open a socket to initiate a traceroute operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

MPLS_OAM_SOCKET_SELECT_FAILED

System Log Message *fec-address*: unable to select socket (*error-message*)

Description The Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) process (mplsoamd) could not select a socket to initiate a traceroute operation.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

MPLS_OAM_TRACEROUTE_INTERRUPTED

System Log Message *fec-address*: topology update interrupted traceroute

Description A traceroute operation was interrupted by a topology change.

Type Event: This message reports an event, not an error

Severity info

Action Wait for the next scheduled traceroute operation.

MPLS_OAM_TTL_EXPIRED

System Log Message *fec-address*: traceroute TTL limit was reached

Description The time-to-live (TTL) limit for the traceroute utility was reached.

Type Error: An error occurred

Severity info

Action Raise the traceroute TTL limit parameter.

MPLS_OAM_UNREACHABLE

System Log Message *fec-address*: traceroute encountered unreachable node

Description The traceroute utility encountered a node that does not have a computable destination address. The Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) process (mplsoamd) therefore could not send a probe to the node.

Type Error: An error occurred

Severity info

Action Contact your technical support representative.

Chapter 50

NEXTHOP System Log Messages

This chapter describes messages with the NEXTHOP prefix. They are generated by the process that decides the next hop.

NEXTHOP_COMPONENTS_LIMIT_REACHED

System Log Message Limit on components reached for flood next hop for routing instance '*routing-instance*'

Description The limit on the number of logical interfaces for a next hop was reached for the indicated routing instance and bridging domain. Only a subset of new interfaces were added to the next hop.

Type Event: This message reports an event, not an error

Severity error

Chapter 51

NSD System Log Messages

This chapter describes messages with the NSD prefix. They are generated by the network security process (nsd), which manages firewall configuration on routers running the JUNOS software with enhanced services.

NSD_MEMORY_ALLOC_FAILED

System Log Message Unable to allocate *count* bytes of memory

Description The network security process (nsd) could not allocate the indicated number of bytes of memory.

Type Error: An error occurred

Severity error

Cause It is possible that system memory is exhausted.

Action Increase the amount of RAM in the Routing Engine.

NSD_RESTART_COMP_CFG_READ_FAILED

System Log Message Subcomponent could not read configuration database

Description As the network security process (nsd) restarted, one or more of its subcomponents could not read its configuration information from configuration database. The nsd process restarted anyway, and routing performance was not affected.

Type Error: An error occurred

Severity error

Chapter 52

PFE System Log Messages

This chapter describes messages with the PFE prefix. They are generated by the Packet Forwarding Engine controller, which manages packet forwarding functions.

PFE_CBF_UNSUPPORTED

System Log Message Internet Processor I does not support CoS-based forwarding

Description The Internet Processor I application-specific integrated circuit (ASIC) does not support class-of-service (CoS)-based forwarding (CBF).

Type Event: This message reports an event, not an error

Severity warning

PFE_FW_DELETE_MISMATCH_ERR

System Log Message Instance mismatch for *type* (*installed-firewall-name* != *deleted-firewall-name*) ifl *logical-interface-index* family *protocol-family*

Description Before a firewall is deleted, it is sanity checked against what is installed in the forwarding topology. A mismatch was detected between the firewall to be deleted and the forwarding topology, and the delete operation was canceled.

Type Error: An error occurred

Severity error

PFE_FW_IF_DIALER_ERR

System Log Message DFW: output *type* (*firewall-name*) on ifl *logical-interface-index* rejected, invalid interface

Description Firewalls that use the ipsec-sa action to forward traffic to an IP Security (IPSec) security association (SA) cannot be configured on the ES Physical Interface Card (PIC) that services the SA. That configuration creates traffic loops within the router and was probably unintended. The problematic filter was automatically removed from the indicated interface.

Type Error: An error occurred

Severity error

PFE_FW_IF_INPUT_ERR

System Log Message DFW: input *type* (*firewall-name*) on ifl *logical-interface-index* rejected, invalid interface

Description Firewalls that use the ipsec-sa action to forward traffic to an IP Security (IPSec) security association (SA) cannot be configured on the ES Physical Interface Card (PIC) that services the SA. That configuration creates traffic loops within the router and was probably unintended. The problematic firewall was automatically removed from the indicated interface.

Type Error: An error occurred

Severity error

PFE_FW_IF_OUTPUT_ERR

System Log Message DFW: output *type* (*firewall-name*) on ifl *logical-interface-index* rejected, invalid interface

Description Firewalls that use the ipsec-sa action to forward traffic to an IP Security (IPSec) security association (SA) cannot be configured on the ES Physical Interface Card (PIC) that services the SA. That configuration creates traffic loops within the router and was probably unintended. The problematic firewall was automatically removed from the indicated interface.

Type Error: An error occurred

Severity error

PFE_FW_PSF_DELETE_MISMATCH_ERR

System Log Message Instance mismatch for *type* (*installed-firewall-name* ! = *deleted-firewall-name*) hardware label *index* family *protocol-family*

Description Before a postservice firewall is deleted, it is sanity checked against what is installed in the forwarding topology. A mismatch was detected between the firewall to be deleted and the forwarding topology, and the delete operation was canceled.

Type Error: An error occurred

Severity error

PFE_FW_SYSLOG_IP

System Log Message FW: *interface-name action protocol-name source-address destination-address source-port-or-type destination-port-or-code* (*count* packets)

Description An IP packet matched against a stateless firewall filter with the indicated 'syslog' action (A = Accept, D = Discard, R = Reject).

Type Event: This message reports an event, not an error

Severity info

PFE_FW_SYSLOG_IP6_GEN

System Log Message FW: *interface-name action protocol-name source-address destination-address* (*count* packets)

Description An IP version 6 (IPv6) packet matched against a stateless firewall filter with the indicated 'syslog' action (A = Accept, D = Discard, R = Reject).

Type Event: This message reports an event, not an error

Severity info

PFE_FW_SYSLOG_IP6_ICMP

System Log Message FW: *interface-name action protocol-name source-address destination-address* type *type* code *error-code* (*count* packets)

Description An IP version 6 (IPv6) Internet Control Message Protocol (ICMP) packet matched against a stateless firewall filter with the indicated 'syslog' action (A = Accept, D = Discard, R = Reject).

Type Event: This message reports an event, not an error

Severity info

PFE_FW_SYSLOG_IP6_TCP_UDP

System Log Message FW: *interface-name action protocol-name source-address destination-address* sport:*source-port* dport:*destination-port* (*count* packets)

Description An IP version 6 (IPv6) Transmission Control Protocol/User Datagram Protocol (TCP/UDP) packet matched against a stateless firewall filter with the indicated 'syslog' action (A = Accept, D = Discard, R = Reject).

Type Event: This message reports an event, not an error

Severity info

PFE_MGCP_ADD_CA_PORT_FAIL

System Log Message Failed to add the MGCP Call Agent port to application definition table

Description Failed to add the MGCP Call Agent port to the application definition table.

Type Error: An error occurred

Severity error

PFE_MGCP_ADD_UA_PORT_FAIL

System Log Message Failed to add the MGCP UA port to application definition table

Description Failed to add the MGCP User Agent port to the application definition table.

Type Error: An error occurred

Severity error

PFE_MGCP_DEL_CA_PORT_FAIL

System Log Message Failed to delete the MGCP Call Agent port from application definition table

Description Failed to remove the MGCP Call Agent port from the application definition table.

Type Error: An error occurred

Severity error

PFE_MGCP_DEL_UA_PORT_FAIL

System Log Message Failed to delete the MGCP User Agent port from application definition table

Description Failed to remove the MGCP User Agent port from the application definition table.

Type Error: An error occurred

Severity error

PFE_MGCP_MEM_INIT_FAILED

System Log Message Failed to create memory pool for *error-message*

Description Failed to initialize the MGCP memory pool.

Type Error: An error occurred

Severity error

PFE_MGCP_REG_HDL_FAIL

System Log Message Failed to register *object-name* handle

Description Failed to register the handler with the external module.

Type Error: An error occurred

Severity error

PFE_NH_RESOLVE_THROTTLED

System Log Message Next-hop resolution requests from interface *logical-interface-index* throttled

Description The Packet Forwarding Engine throttled next-hop resolution requests from the indicated interface, because the high number of requests might constitute an attempted denial-of-service (DoS) attack. Examples of events that generate next-hop resolution requests include an attempt to forward a packet without an Address Resolution Protocol (ARP) entry and receiving a multicast data packet with no matching route. Normally, the Packet Forwarding Engine forwards the requests to the Routing Engine.

Type Event: This message reports an event, not an error

Severity info

PFE_SCCP_ADD_PORT_FAIL

System Log Message Failed to add SCCP ALG port to application definition table

Description Failed to add the SCCP port to the application definition table.

Type Error: An error occurred

Severity error

PFE_SCCP_DEL_PORT_FAIL

System Log Message Failed to remove SCCP ALG port from application definition table

Description Failed to delete the SCCP port from application definition table.

Type Error: An error occurred

Severity error

PFE_SCCP_REG_NAT_VEC_FAIL

System Log Message Failed to add SCCP ALG vector to flow module

Description Failed to register the SCCP vector with the flow module.

Type Error: An error occurred

Severity error

PFE_SCCP_REG_RM_FAIL

System Log Message Failed to register SCCP client to Resource Manager

Description Failed to register the SCCP Resource Manager client.

Type Error: An error occurred

Severity error

PFE_SCCP_REG_VSIP_FAIL

System Log Message Failed to register SCCP client to VoIP State IP port

Description Failed to register the SCCP client to VoIP State IP port.

Type Error: An error occurred

Severity error

PFE_SCCP_RM_CLIENTID_FAIL

System Log Message Failed to get SCCP Resource Manager client identifier

Description Failed to get the SCCP Resource Manager client identifier.

Type Error: An error occurred

Severity error

PFE_SCREEN_CFG_ERROR

System Log Message fail to *operation* the screen config due to *error-message*

Description faile to change the configuration of screen module

Type Error: An error occurred

Severity error

PFE_SCREEN_CFG_EVENT

System Log Message [*operation*]: screen name - *context-name*

Description configuration of screen module is changed

Type Event: This message reports an event, not an error

Severity info

PFE_SCREEN_MT_CFG_ERROR

System Log Message failed to *operation* the screen config due to *error-message*

Description failed to change the configuration of screen module

Type Error: An error occurred

Severity error

PFE_SCREEN_MT_CFG_EVENT

System Log Message [*operation*]: screen name - *context-name*

Description configuration of screen module is changed

Type Event: This message reports an event, not an error

Severity info

PFE_SIP_ADD_PORT_FAIL

System Log Message Failed to add SIP ALG port to application definition table

Description Failed to add the SIP port to the application definition table.

Type Error: An error occurred

Severity error

PFE_SIP_DEL_PORT_FAIL

System Log Message Failed to delete SIP ALG port from application definition table

Description Failed to remove the SIP port from the application definition table.

Type Error: An error occurred

Severity error

PFE_SIP_MEM_INIT_FAILED

System Log Message Failed to create memory pool for *object-name*

Description Failed to create a memory pool for SIP.

Type Error: An error occurred

Severity error

PFE_SIP_REG_HDL_FAIL

System Log Message Failed to register *object-name* handle

Description Failed to register the handler with the external module.

Type Error: An error occurred

Severity error

PFE_USP_TRACE_BUFFER_CREATE

System Log Message USP Trace buffer created for *identifier*.

Description The USP Packet Forwarding Engine (PFE) created a trace buffer for the indicated identifier.

Type Event: This message reports an event, not an error

Severity info

PFE_USP_TRACE_BUFFER_DELETE

System Log Message Deleting USP trace buffer for *identifier*.

Description The USP Packet Forwarding Engine (PFE) deleted a trace buffer for the indicated identifier.

Type Event: This message reports an event, not an error

Severity info

PFE_USP_TRACE_BUFFER_LIMIT

System Log Message Number of buffered records limited to *requested-size* for *identifier*.

Description The USP Packet Forwarding Engine (PFE) trace buffers were limited to the indicated size for the indicated identifier.

Type Event: This message reports an event, not an error

Severity info

PFE_USP_TRACE_BUFFER_MEM_FAIL

System Log Message Cannot allocate buffer to hold *requested-size* records for *identifier*.

Description The USP Packet Forwarding Engine (PFE) did not allocate buffers of the indicated size for the indicated identifier.

Type Error: An error occurred

Severity error

PFE_USP_TRACE_BUFFER_MODIFY

System Log Message USP Trace buffer modified for *identifier*.

Description The USP Packet Forwarding Engine (PFE) modified trace buffers for the indicated identifier.

Type Event: This message reports an event, not an error

Severity info

Chapter 53

PFED System Log Messages

This chapter describes messages with the PFED prefix. They are generated by the Packet Forwarding Engine process, which gathers and reports Packet Forwarding Engine statistics.

PFED_NOTIFICATION_STATS_FAILED

System Log Message Unable to retrieve notification statistics

Description The Packet Forwarding Engine process (pfed) could not retrieve Packet Forwarding Engine notification statistics.

Type Error: An error occurred

Severity warning

Chapter 54

PGCPD System Log Messages

This chapter describes messages with the PGCPD prefix. They are generated by the pgcpd process, which decodes packet gateway control protocol (pgcp) messages that virtual packet gateways (vpg) receive from the packet gateway controller (pgc) and translates the pgcp messages to inter-process communication (ipc) messages.

PGCPD_BGF_FAILED_RECONNECT

System Log Message BGF [*index*] Failed to Reconnected with SPDF <*index1*>

Description The BGF was registered with the SPDF, became disconnected, sent a DC/900 service-change to that PGC, and received a rejection or the request has timed out

Type Event: This message reports an event, not an error

Severity warning

PGCPD_BGF_FAILED_REGISTERED

System Log Message BGF [*index*] Failed to Register with SPDF <*index1*>

Description The BGF failed to register with <SPDF> and received reject or timeout

Type Error: An error occurred

Severity warning

PGCPD_BGF_FAILURE

System Log Message The BGF[*index*] is now out-of-service

Description The BGF which was in-service, has now moved to out-of-service

Type Error: An error occurred

Severity error

PGCPD_BGF_NETWORK_DISCONNECT

System Log Message BGF [*index*] Was Disconnected

Description The BGF was disconnected from the SPDF due to a network disruption

Type Event: This message reports an event, not an error

Severity warning

PGCPD_BGF_RECONNECT

System Log Message BGF [*index*] Reconnected with SPDF <*index1*>

Description The BGF was registered with the SPDF, became disconnected, sent a DC/900 service-change to that PGC and received a confirmation reply

Type Event: This message reports an event, not an error

Severity notice

PGCPD_BGF_REGISTERED

System Log Message BGF [*index*] is Registered Successfully with SPDF <*index1*>

Description The BGF registered successfully with <SPDF>

Type Event: This message reports an event, not an error

Severity notice

PGCPD_BGF_SHUTDOWN_FORCED

System Log Message The BGF[*index*] is now out-of-service administrative forced shutdown

Description The BGF which was in-service, has now moved to out-of-service due to an administrative forced shutdown

Type Event: This message reports an event, not an error

Severity notice

PGCPD_BGF_SHUTDOWN_GRACE

System Log Message The BGF [*index*] is now out-of-service administrative graceful shutdown

Description The BGF which was in-service, has now moved to out-of-service due to an administrative graceful shutdown

Type Event: This message reports an event, not an error

Severity notice

PGCPD_BGF_SHUTDOWN_PIC_DISABLED

System Log Message The BGF [*index*] is now out-of-service PIC administrative disable

Description The BGF which was in-service, has now moved to out-of-service due to an administrative PIC disabled

Type Event: This message reports an event, not an error

Severity notice

PGCPD_BGF_STARTUP

System Log Message The BGF[*index*] is now in-service

Description The BGF which was out-of-service, is now in-service

Type Event: This message reports an event, not an error

Severity notice

PGCPD_GATE_RATE_LIMIT_ERR

System Log Message Limit violation occurred on gate Id = *index*

Description The gate has a rate limit violation

Type Error: An error occurred

Severity info

PGCPD_MEDIA_INACTIVITY

System Log Message no RTP media packets arrived so media is inactive Gate Id = *index*

Description The media is inactive because no RTP media packets arrived.

Type Error: An error occurred

Severity info

PGCPD_REMOTE_SRC_ADDR_SET

System Log Message Manager received gate latch-done notification Gate Id = *index*

Description Set the source address from the packet as the gate remote source address.

Type Event: This message reports an event, not an error

Severity info

PGCPD_SHUTDOWN

System Log Message The pgcpd process shut down

Description The packet gateway control process (pgcpd) state was shut down.

Type Event: This message reports an event, not an error

Severity notice

PGCPD_STARTUP

System Log Message The pgcpd process just started up

Description The packet gateway control process (pgcpd) just started up

Type Event: This message reports an event, not an error

Severity notice

PGCPD_SWITCH_OVER

System Log Message switch over

Description Switch over from active to backup Routing Engine

Type Event: This message reports an event, not an error

Severity warning

Chapter 55

PING System Log Messages

This chapter describes messages with the PING prefix. They are generated by the ping command, which tests whether a remote machine is accessible across the network.

PING_EGRESS_JITTER_THRESH_EXCEED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The jitter for the egress trip time exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_EGRESS_STDDEV_THRESH_EXCEED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The standard deviation of the egress trip time exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_EGRESS_THRESHOLD_EXCEEDED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The egress trip time measured for a probe exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_INGRESS_JTR_THRESH_EXCEED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The jitter for the ingress trip time exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_INGRESS_STDDV_THRESH_EXCEED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The standard deviation of the ingress trip time exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_INGRESS_THRESHOLD_EXCEEDED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The ingress trip time measured for a probe exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_PROBE_FAILED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The number of successive probe failures exceeded the pingCtlTrapProbeFailureFilter threshold.

Type Event: This message reports an event, not an error

Severity info

PING_RTT_JTR_THRESH_EXCEED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The jitter for the round trip time exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_RTT_STDDV_THRESH_EXCEED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The standard deviation of the round trip time exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_RTT_THRESHOLD_EXCEEDED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description The round trip time measured for a probe exceeded the configured threshold during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

PING_TEST_COMPLETED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description All probes were sent and the number of failed probes was less than the pingCtlTrapTestFailureFilter threshold.

Type Event: This message reports an event, not an error

Severity info

PING_TEST_FAILED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description All probes were sent but the number of failed probes equaled or exceeded the pingCtlTrapTestFailureFilter threshold.

Type Event: This message reports an event, not an error

Severity info

PING_UNKNOWN_THRESH_TYPE_EXCEED

System Log Message pingCtlOwnerIndex = *test-owner*, pingCtlTestName = *test-name*

Description An unknown type of threshold event was reported during the indicated test conducted by the indicated user.

Type Event: This message reports an event, not an error

Severity info

Chapter 56

PPMD System Log Messages

This chapter describes messages with the PPMD prefix. They are generated by the periodic packet management process (ppmd), which maintains routing protocol adjacencies for the routing protocol process (rpd).

PPMD_ASSERT_SOFT

System Log Message Soft assertion failed at line *line-number* in file '*source-filename*' with error "*message*", but ppmd with PID *pid* continued running

Description The source code for the periodic package management process (ppmd) includes internal self-consistency checks. As the ppmd process with the indicated process ID (PID) executed the binary compiled from the indicated source file, a check failed at the indicated line number in the file. The ppmd process created a diagnostic core file for analysis by technical support personnel and continued to run.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Examine the messages that immediately follow this message in the system log for information about possible causes. Contact a technical support representative, and be ready to provide the list of messages and the diagnostic core file, if requested.

PPMD_OPEN_ERROR

System Log Message *function-name*: open error on pipe to *protocol-name* (*error-message*)

Description The periodic packet management process (ppmd) could not initialize the indicated protocol.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

PPMD_READ_ERROR

System Log Message Read error on pipe from *protocol-name*: *reason* (*error-message*)

Description The periodic packet management process (ppmd) could not read a message on a pipe for the indicated protocol.

Type Error: An error occurred

Severity info

Action Contact your technical support representative.

PPMD_WRITE_ERROR

System Log Message *function-name*: write error on pipe to *protocol-name* (*error-message*)

Description The periodic packet management process (ppmd) could not write a message on a pipe for the indicated protocol.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

Chapter 57

PPPD System Log Messages

This chapter describes messages with the PPPD prefix. They are generated by the Point-to-Point Protocol (PPP) process (pppd), which processes packets that use PPP.

PPPD_AUTH_CREATE_FAILED

System Log Message Unable to allocate authentication handle: *error-message*

Description The Point-to-Point Protocol process (pppd) could not allocate an authentication object, for the indicated reason.

Type Error: An error occurred

Severity error

PPPD_CHAP_AUTH_IN_PROGRESS

System Log Message Interface *interface-name* received response '*operation*' with CHAP ID *message-id*, but was still authenticating previous response

Description The Point-to-Point Protocol process (pppd) received another Challenge Handshake Authentication Protocol (CHAP) response from a peer while authenticating a previous CHAP response sent by that peer. The peer is resending CHAP responses faster than the pppd process can process them.

Type Error: An error occurred

Severity error

PPPD_CHAP_GETHOSTNAME_FAILED

System Log Message *interface-name*: Unable to obtain hostname for outgoing CHAP message: *error-message*

Description The Point-to-Point Protocol process (pppd) could not obtain the hostname needed to fill in the 'Name' field in an outgoing CHAP packet.

Type Error: An error occurred

Severity error

PPPD_CHAP_INVALID_IDENTIFIER

System Log Message Interface *interface-name* received '*operation*' message with CHAP ID *message-id* instead of expected ID *expected-value*

Description The Point-to-Point Protocol process (pppd) received a Challenge Handshake Authentication Protocol (CHAP) message from a peer that included the indicated message identifier, which did not match the indicated expected value.

Type Error: An error occurred

Severity info

PPPD_CHAP_INVALID_OPCODE

System Log Message *interface-name*: received invalid operation code *operation* (type *operation-code*, CHAP ID *message-id*)

Description The Point-to-Point Protocol process (pppd) received a Challenge Handshake Authentication Protocol (CHAP) message that included the indicated operation code, which is invalid.

Type Error: An error occurred

Severity error

PPPD_CHAP_LOCAL_NAME_UNAVAILABLE

System Log Message Unable to determine value for 'Name' in outgoing CHAP packet

Description The Point-to-Point Protocol process (pppd) could not determine the value needed to fill in the 'Name' field in an outgoing Challenge Handshake Authentication Protocol (CHAP) packet, because either the local name was not specified or pppd could not determine the hostname.

Type Error: An error occurred

Severity error

PPPD_CHAP_OPERATION_UNEXPECTED

System Log Message *interface-name*: unexpected operation type *operation* (CHAP ID *message-id*)

Description The Challenge Handshake Authentication Protocol (CHAP) message with the indicated identifier had the indicated operation type, which the Point-to-Point Protocol process (pppd) did not expect.

Type Error: An error occurred

Severity info

PPPD_CHAP_REPLAY_ATTACK_DETECTED

System Log Message *interface-name*: received *operation* with CHAP ID *message-id*, which is identical to an outstanding challenge. Peer is trying to exhort response value.

Description During an exchange of authentication messages, a peer responded to a challenge message from the Point-to-Point Protocol process (pppd) by returning the same message. The pppd process did not respond to the peer, because doing so would provide the answer to the original challenge. The peer must provide the answer on its own for authentication to succeed.

Type Error: An error occurred

Severity error

PPPD_EVLIB_CREATE_FAILURE

System Log Message Unable to create event context: *error-message*

Description The Point-to-Point Protocol process (pppd) could not create a context for handling asynchronous events, for the indicated reason.

Type Error: An error occurred

Severity error

PPPD_LOCAL_CREATE_FAILED

System Log Message Unable to allocate LOCAL module handle: *error-message*

Description The Point-to-Point Protocol process (pppd) attempted to allocate a locally configured 'password' authentication module as part of its authentication sequence. The allocation failed.

Type Error: An error occurred

Severity error

PPPD_MEMORY_ALLOCATION_FAILURE

System Log Message Unable to allocate memory for object *object-name*: *error-message*

Description The Point-to-Point Protocol process (pppd) could not allocate memory from the heap for the indicated object.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

PPPD_PAP_GETHOSTNAME_FAILED

System Log Message Unable to obtain hostname for PAP message sent from interface *interface-name*: *error-message*

Description The Point-to-Point Protocol process (pppd) could not obtain the hostname it needed to fill in the 'Name' field in an outgoing Password Authentication Protocol (PAP) packet sent from the indicated interface.

Type Error: An error occurred

Severity error

PPPD_PAP_INVALID_IDENTIFIER

System Log Message Interface *interface-name* received '*operation*' message with PAP ID *message-id* instead of expected ID *expected-value*

Description The Point-to-Point Protocol process (pppd) received a Password Authentication Protocol (PAP) message from a peer that included the indicated identifier, which did not match the indicated expected value.

Type Error: An error occurred

Severity info

PPPD_PAP_INVALID_OPCODE

System Log Message Interface *interface-name* received '*operation*' message with PAP ID *message-id* and invalid operation code *operation-code*

Description The Point-to-Point Protocol process (pppd) received a Password Authentication Protocol (PAP) message from a peer that included the indicated operation code, which is invalid.

Type Error: An error occurred

Severity error

PPPD_PAP_LOCAL_PASSWORD_UNAVAIL

System Log Message Unable to determine value for 'Password' in outgoing PAP packet

Description The Point-to-Point Protocol process (pppd) could not determine the value to write in the 'Password' field in an outgoing Password Authentication Protocol (PAP) packet.

Type Error: An error occurred

Severity error

Cause The local password was not defined for the local hostname.

PPPD_PAP_OPERATION_UNEXPECTED

System Log Message *interface-name*: unexpected operation type *operation* (PAP ID *message-id*)

Description The Point-to-Point Protocol process (pppd) received a Password Authentication Protocol (PAP) message with the indicated identifier and operation type. The operation type was not valid.

Type Error: An error occurred

Severity info

PPPD_POOL_ADDRESSES_EXHAUSTED

System Log Message No addresses available in pool "*pool-name*" to assign to remote peer on interface *interface-name*

Description The Point-to-Point Protocol process (pppd) could not assign an address from the indicated address pool to the remote peer on the indicated interface, because there were no more addresses available in the pool.

Type Error: An error occurred

Severity error

Action Increase the number of addresses in the address pool.

PPPD_RADIUS_ADD_SERVER_FAILED

System Log Message Unable to add RADIUS server *radius-server* for profile *access-profile*: *error-message*

Description The Point-to-Point Protocol process (pppd) could not add the indicated RADIUS server for the indicated access profile.

Type Error: An error occurred

Severity error

PPPD_RADIUS_ALLOC_PASSWD_FAILED

System Log Message Unable to allocate RADIUS password of size *size*: *error-message*

Description The Point-to-Point Protocol process (pppd) could not allocate space for a temporary Challenge Handshake Authentication Protocol (CHAP) RADIUS password of the indicated size.

Type Error: An error occurred

Severity error

PPPD_RADIUS_CREATE_FAILED

System Log Message Unable to allocate RADIUS module handle: *error-message*

Description The Point-to-Point Protocol process (pppd) attempted to allocate a RADIUS authentication module as part of its authentication sequence. The allocation failed.

Type Error: An error occurred

Severity error

PPPD_RADIUS_CREATE_REQ_FAILED

System Log Message Unable to create RADIUS access request message: *error-message*

Description The Point-to-Point Protocol process (pppd) could not create an access request message to send to the RADIUS server.

Type Error: An error occurred

Severity error

PPPD_RADIUS_GETHOSTNAME_FAILED

System Log Message Unable to obtain hostname for outgoing RADIUS message: *error-message*

Description The Point-to-Point Protocol process (pppd) could not obtain the hostname it needed to fill in the PPP_IDENTIFIER field in an outgoing RADIUS message.

Type Error: An error occurred

Severity error

PPPD_RADIUS_MESSAGE_UNEXPECTED

System Log Message Unknown response from RADIUS server: *return-value*

Description The RADIUS authentication module for the Point-to-Point Protocol process (pppd) received a message from the RADIUS server that it could not process.

Type Error: An error occurred

Severity error

PPPD_RADIUS_NO_VALID_SERVERS

System Log Message Unable to find valid RADIUS server for profile *access-profile*

Description The Point-to-Point Protocol process (pppd) could not access a valid RADIUS server to use for the indicated access profile.

Type Error: An error occurred

Severity error

PPPD_RADIUS_OPEN_FAILED

System Log Message rad_auth_open failed: *error-message*

Description The Point-to-Point Protocol process (pppd) could not create a RADIUS object handle, which it uses to communicate with the RADIUS server.

Type Error: An error occurred

Severity error

PPPD_RADIUS_ROUTE_INST_ENOENT

System Log Message Ignored RADIUS server *radius-server* for profile *access-profile* because routing instance *routing-instance* did not exist

Description The indicated routing instance, which the Point-to-Point Protocol process (pppd) uses for routing of RADIUS packets, was not defined.

Type Event: This message reports an event, not an error

Severity notice

Cause The process of adding the required routing instance was still in progress when the message was logged.

Action None required. Authentication with the indicated RADIUS server is automatically reattempted, and can succeed when the interface exists.

Chapter 58

PROFILER System Log Messages

This chapter describes messages with the PROFILER prefix. They are generated by the profiler service process (profilerd).

PROFILER_RECONFIGURE_SIGHUP

System Log Message SIGHUP - re-reading configuration

Description In response to a SIGHUP signal, the profiler service process (profilerd) read its configuration from the configuration database

Type Event: This message reports an event, not an error

Severity info

Chapter 59

RDD System Log Messages

This chapter describes messages with the RDD prefix. They are generated by the redundant interfaces process (rdd), which manages redundant interfaces when they are configured on Adaptive Services Physical Interface Cards (PICs).

RDD_EVLIB_CREATE_FAILURE

System Log Message evCreate failed (*error-message*)

Description The redundant interfaces process (rdd) could not create a context used for handling all asynchronous events (such as timers and message availability).

Type Error: An error occurred

Severity emergency

RDD_IFDEV_ADD_FAILURE

System Log Message *function-name*: unable to add interface device *interface-name* (*error-message*)

Description The redundant interfaces process (rdd) could not create an interface device because an error occurred during the indicated call to the routing socket library.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RDD_IFDEV_DELETE_FAILURE

System Log Message *function-name*: rtslib delete operation failed for interface device *interface-name* (*error-message*)

Description The redundant interfaces process (rdd) could not delete an interface device because an error occurred during the indicated call to the routing socket library.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RDD_IFDEV_GET_FAILURE

System Log Message *function-name*: rtslib get operation failed for interface device *interface-name* (*error-message*)

Description The redundant interfaces process (rdd) could not get an interface device because an error occurred during the indicated call to the routing socket library.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RDD_IFDEV_INCOMPATIBLE_REVERT

System Log Message *function-name*: did not revert *rsp-interface-name* back to primary interface *primary-interface-name*; PIC is incompatible with secondary

Description The redundant interfaces process (rdd) tried to migrate service processing for the indicated redundant interface from the secondary interface back to the indicated primary interface. The attempt failed because the Adaptive Services (AS) Physical Interface Cards (PICs) that house the primary and secondary interfaces are not compatible.

Type Error: An error occurred

Severity error

RDD_IFDEV_INCOMPATIBLE_SWITCH

System Log Message Unable to switch *rsp-interface-name* to secondary interface *secondary-interface-name*; PIC is incompatible with primary

Description The redundant interfaces process (rdd) tried to migrate service processing for the indicated redundant interface from the primary interface to the indicated secondary interface. The attempt failed because the Adaptive Services (AS) Physical Interface Cards (PICs) that house the primary and secondary interfaces are not compatible.

Type Error: An error occurred

Severity error

RDD_IFDEV_RETRY_NOTICE

System Log Message *function-name*: repeated attempt to add interface device *interface-name* failed (*error-message*)

Description The redundant interfaces process (rdd) tried repeatedly to create the indicated interface device, but the attempts failed. After generating this message, rdd waited a while for resources to free up and tried again.

Type Event: This message reports an event, not an error

Severity warning

Cause Necessary resources might have been unavailable. They should become available soon.

RDD_NEW_INTERFACE_STATE

System Log Message Event *event-name* changed state of interface *interface-name* from '*old-state*' to '*new-state*'

Description The indicated event on the indicated redundant interface changed the interface state as indicated.

Type Event: This message reports an event, not an error

Severity info

RDD_TRACE_FILE_OPEN_FAILED

System Log Message trace_file_open() failed: *error-message*

Description The redundant interfaces process (rdd) could not open the file in which it records log and trace messages.

Type Error: An error occurred

Severity error

Chapter 60

RMOPD System Log Messages

This chapter describes messages with the RMOPD prefix. They are generated by the Simple Network Management Protocol (SNMP) remote operations process (rmopd), which services SNMP requests for execution of ping and traceroute operations.

RMOPD_ADDRESS_MULTICAST_INVALID

System Log Message Multicast address is not allowed

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it can specify the addresses of the source and target hosts for the operation. A request failed because the client specified a multicast address for either or both the source and target hosts.

Type Error: An error occurred

Severity error

RMOPD_ADDRESS_SOURCE_INVALID

System Log Message Source address invalid: *error-message*

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it can specify the address to use as the source host for the operation, along with the corresponding address type (such as IP version 4 [IPv4]). Either the specified address was invalid because it did not match the specified address type, or the address could not be resolved.

Type Error: An error occurred

Severity notice

RMOPD_ADDRESS_STRING_FAILURE

System Log Message Unable to convert numeric address to string: *error-message*

Description The remote Simple Network Management Protocol (SNMP) operations process (rmopd) could not convert a numeric host address to the corresponding hostname text string.

Type Error: An error occurred

Severity error

RMOPD_ADDRESS_TARGET_INVALID

System Log Message rmop_util_set_address status message: *error-message*

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it must specify the address of the target host along with the corresponding address type (such as IP version 4 [IPv4]). Either the specified address was invalid because it did not match the specified address type, or the address could not be resolved.

Type Error: An error occurred

Severity error

RMOPD_ICMP_ADDR_TYPE_UNSUPPORTED

System Log Message Only IPv4 source address is supported

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it can specify the address type (such as IP version 4 [IPv4]) of the source and target hosts for the operation. The client specified an unsupported address type.

Type Error: An error occurred

Severity error

RMOPD_IFINDEX_NOT_ACTIVE

System Log Message ifindex: *snmp-interface-index*

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it can specify which interface to use as the source host address, identifying it by either its numerical index or its name. The indicated index was invalid because it represents an inactive interface.

Type Error: An error occurred

Severity error

RMOPD_IFINDEX_NO_INFO

System Log Message No information for *snmp-interface-index*, message: *error-message*

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it can specify which interface to use as the source host address, identifying it by either its numerical index or its name. The SNMP remote operations process (rmopd) could not find any information about the interface with the indicated index.

Type Error: An error occurred

Severity error

RMOPD_IFNAME_NOT_ACTIVE

System Log Message ifname: *interface-name*

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it can specify which interface to use as the source host address, identifying it by either its numerical index or its name. The indicated name was invalid because it represents an inactive interface.

Type Error: An error occurred

Severity error

RMOPD_IFNAME_NO_INFO

System Log Message No information for *interface-name*, message: *error-message*

Description When a Simple Network Management Protocol (SNMP) client requests a remote operation, it can specify which interface to use as the source host address, identifying it by either its numerical index or its name. The SNMP remote operations process (rmopd) could not find any information about the interface with the indicated name.

Type Error: An error occurred

Severity error

RMOPD_ROUTING_INSTANCE_NO_INFO

System Log Message No information for routing instance *routing-instance*: *error-message*

Description The indicated routing instance does not exist, so the Simple Network Management Protocol (SNMP) remote operations process (rmopd) could not retrieve information about it.

Type Error: An error occurred

Severity error

RMOPD_TRACEROUTE_ERROR

System Log Message Message: *error-message*

Description The traceroute application reported the indicated error message to the Simple Network Management Protocol (SNMP) remote operations process (rmopd).

Type Error: An error occurred

Severity notice

Chapter 61

RPD System Log Messages

This chapter describes messages with the RPD prefix. They are generated by the routing protocol process (rpd), which controls the routing protocols that run on the routing platform.

RPD_ABORT

System Log Message abort *executable-name*[*pid*] version *version* built by *builder* on *date*: *error-message*

Description The routing protocol process (rpd) terminated because of an internal error.

Type Error: An error occurred

Severity error

Action Examine the messages that immediately follow this message in the system log for information about possible causes.

Cause An internal software failure occurred.

RPD_ACTIVE_TERMINATE

System Log Message Exiting with active tasks: *task-name*

Description After receiving multiple termination requests, the routing protocol process (rpd) exited without performing the indicated cleanup tasks.

Type Event: This message reports an event, not an error

Severity notice

RPD_ASSERT

System Log Message Assertion failed *executable-name*[*pid*]: file "*source-filename*", line *line-number*: "*message*"

Description The source code for the routing protocol process (rpd) includes internal self-consistency checks. A check failed at the indicated line number in the indicated source file, causing the instance of rpd that was using the indicated binary and had the indicated process ID (PID) to terminate. The process created a diagnostic core dump for analysis by technical support personnel.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Examine the messages that immediately follow this message in the system log for information about possible causes. Contact a technical support representative, and be ready to provide the list of messages and the diagnostic core dump, if requested.

RPD_ASSERT_SOFT

System Log Message Soft assertion failed *executable-name*[*pid*]: file "*source-filename*", line *line-number*: "*message*", daemon continued running

Description The source code for the routing protocol process (rpd) includes internal self-consistency checks. A check failed at the indicated line number in the indicated source file, but the instance of rpd that was using the indicated binary and had the indicated process ID (PID) continued running. The process created a diagnostic core dump for analysis by technical support personnel.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Examine the messages that immediately follow this message in the system log for information about possible causes. Contact a technical support representative, and be ready to provide the list of messages and the diagnostic core dump, if requested.

RPD_BFD_READ_ERROR

System Log Message Read error on pipe from bfdd: *reason* (*error-message*)

Description The routing protocol process (rpd) could not read a message available on the read pipe from the Bidirectional Forwarding Detection process (bfdd).

Type Error: An error occurred

Severity info

Action Contact your technical support representative.

RPD_BFD_WRITE_ERROR

System Log Message *function-name*: write error on pipe to bfdd (*error-message*)

Description The routing protocol process (rpd) could not write a message on the pipe to the Bidirectional Forwarding Detection process (bfdd).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_BGP_NEIGHBOR_STATE_CHANGED

System Log Message BGP peer *peer-name* changed state from *old-state* to *new-state* (event *event-type*)

Description During BGP negotiation with the local router, the state of the indicated BGP neighbor (peer) changed as indicated. The ESTABLISHED state is the final state in the neighbor negotiation.

Type Event: This message reports an event, not an error

Severity warning

RPD_DYN_CFG_BAD_REQ_OPCODE

System Log Message Received unexpected dynamic config opcode *operation-code*

Description The routing protocol process (rpd) received a dynamic configuration request with an unexpected operation code.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_BUSY_SIGNAL_FAILED

System Log Message Dynamic config *action* busy signal failed: *error-message*

Description The routing protocol process (rpd) failed to notify dynamic configuration clients about its availability to process dynamic configuration requests.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_DYN_CFG_GET_PROFILE_FAILED

System Log Message Get dynamic profiles failed: *error-code*

Description The routing protocol process (rpd) tried to load a profile from the database and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_GET_PROF_NAME_FAILED

System Log Message Get profile name for session *client-session-id* failed: *error-code*

Description The routing protocol process (rpd) tried to get the profile name from the session snapshot and failed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_DYN_CFG_GET_SES_STATE_FAILED

System Log Message Get session state for session *client-session-id* failed: *error-code*

Description The routing protocol process (rpd) failed to get the session state from the session snapshot.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_DYN_CFG_GET_SNAPSHOT_FAILED

System Log Message Get session id *client-session-id* snapshot failed: *error-code*

Description The routing protocol process (rpd) tried to load client session data from the database and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_PDB_CLOSE_FAILED

System Log Message Failed to close profile database: *error-code*

Description The routing protocol process (rpd) tried to close the profile database and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_PDB_OPEN_FAILED

System Log Message Failed to open profile database: *error-code*

Description The routing protocol process (rpd) tried to open the profile database and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_PROCESSING_FAILED

System Log Message Module *module* failed to process dynamic configuration

Description The routing protocol process (rpd) tried to process dynamic configuration and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_REGISTER_FAILED

System Log Message Dynamic config registration failed: *error-message*

Description The routing protocol process (rpd) tried to register with the dynamic configuration subsystem and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_REQUEST_ACK_FAILED

System Log Message Failed to ack request *data-id*: *error-code*

Description The routing protocol process (rpd) tried to acknowledge a dynamic configuration request and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_SCHEMA_OPEN_FAILED

System Log Message Could not open configuration schema: *error-message*

Description The routing protocol process (rpd) tried to open the configuration schema and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_SDB_CLOSE_FAILED

System Log Message Failed to close session database: *error-code*

Description The routing protocol process (rpd) tried to close the session database and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_SDB_OPEN_FAILED

System Log Message Failed to open session database: *error-code*

Description The routing protocol process (rpd) tried to open the session database and failed.

Type Error: An error occurred

Severity error

RPD_DYN_CFG_SET_CONTEXT_FAILED

System Log Message Set dynamic config context for profile *profile-name* session *client-session-id*ailed

Description The routing protocol process (rpd) tried to set up the dynamic configuration context and failed.

Type Error: An error occurred

Severity error

RPD_ESIS_ADJDOWN

System Log Message ES-IS lost *adjacency-type* adjacency to *neighbor-nsap-net*n on *interface-name*, reason: *reason*

Description An ES-IS adjacency with the indicated neighboring router was terminated. The local router no longer exchanges routing information with, or directs traffic to, the neighboring router.

Type Event: This message reports an event, not an error

Severity notice

Cause The communication path to the neighboring router was disrupted, a protocol error occurred, or the neighboring router was powered down.

RPD_ESIS_ADJUP

System Log Message ES-IS new *adjacency-type* adjacency to *neighbor-nsap-net*n on *interface-name*

Description An ES-IS adjacency was established with the indicated neighboring router. The local router can now exchange information with it.

Type Event: This message reports an event, not an error

Severity info

RPD_EXIT

System Log Message Exit *executable-name*[*pid*] version *version* built by *builder* on *date*, caller *address*

Description The routing protocol process (rpd) exited, either in response to a user request or because of a system error.

Type Event: This message reports an event, not an error

Severity notice

Cause A system resource was unavailable, rpd did not understand an error, or a user terminated the process.

Action Examine the messages that immediately follow this message in the system log for information about possible causes.

RPD_IFD_INDEXCOLLISION

System Log Message Physical interface collision -- same name, different index (new *new-interface-name new-index* old *old-interface-name old-value*)

Description The routing protocol process (rpd) received a message from the kernel in which the numerical index associated with the indicated interface name differed from the index-to-name mapping maintained by rpd.

Type Error: An error occurred

Severity error

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_IFD_NAMECOLLISION

System Log Message Physical interface collision -- different name, same index (new *new-interface-name new-index*, old *old-interface-name old-value*)

Description The routing protocol process (rpd) received a message from the kernel in which the name associated with the indicated numerical interface index differed from the name-to-index mapping maintained by rpd.

Type Error: An error occurred

Severity error

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_IFL_INDEXCOLLISION

System Log Message Logical interface collision -- same name, different index (new *new-interface-name new-index* old *old-interface-name old-value*)

Description The routing protocol process (rpd) received a message from the kernel in which the numerical index associated with the indicated interface name differed from the index-to-name mapping maintained by rpd.

Type Error: An error occurred

Severity error

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_IFL_NAMECOLLISION

System Log Message Logical interface collision -- different name, same index (new *new-interface-name new-index*, old *old-interface-name old-value*)

Description The routing protocol process (rpd) received a message from the kernel in which the name associated with the indicated numerical interface index differed from the name-to-index mapping maintained by rpd.

Type Error: An error occurred

Severity error

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_IGMP_ACCOUNTING_OFF

System Log Message *interface-name time*

Description Internet Group Management Protocol (IGMP) accounting for the indicated interface was disabled at the indicated time.

Type Event: This message reports an event, not an error

Severity info

RPD_IGMP_ACCOUNTING_ON

System Log Message *interface-name time*

Description Internet Group Management Protocol (IGMP) accounting for the indicated interface was enabled at the indicated time.

Type Event: This message reports an event, not an error

Severity info

RPD_IGMP_ALL_SUBSCRIBERS_DELETED

System Log Message All subscribers on interface *interface-name* deleted at *time* because the interface is down

Description IGMP interface down event.

Type Event: This message reports an event, not an error

Severity info

RPD_IGMP_CFG_CREATE_ENTRY_FAILED

System Log Message Could not create entry for *entry*.

Description Internet Group Management Protocol (IGMP) failed to create the indicated configuration entry. The configuration request failed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_IGMP_CFG_INVALID_VALUE

System Log Message The *object-name* configuration object *identifier* field has an invalid value of *value*

Description The configuration request failed because the indicated configuration object contained the indicated invalid value.

Type Error: An error occurred

Severity error

Action Modify configuration statement to use a valid value.

RPD_IGMP_DYN_CFG_INVALID_STMT

System Log Message Invalid dynamic configuration statement: *configuration-statement*

Description The indicated dynamic configuration statement was invalid. The dynamic configuration instantiation request was rejected.

Type Error: An error occurred

Severity error

Action Remove the unsupported configuration statement.

RPD_IGMP_DYN_CFG_SES_ID_MISMATCH

System Log Message Dynamic configuration entry for interface *interface-name* with session id *client-session-id* found an existing entry with a different session id of *client-session-id-1*.

Description The dynamic configuration instantiation request matched an existing dynamic configuration block that had a different session id. The dynamic configuration instantiation request was rejected.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_IGMP_JOIN

System Log Message Listener *source-address* sent a join to *destination-address* for group *group-address* source *sender-address* on interface *interface-name* at *time*

Description IGMP join event.

NOTE: The *destination address* field for RPD_IGMP_JOIN is no longer valid. To remove any processing impact relating to this message, the string “(null)” has been substituted for the destination address.

Type Event: This message reports an event, not an error

Severity info

RPD_IGMP_LEAVE

System Log Message Listener *source-address* sent a leave to *destination-address* for group *group-address* source *sender-address* on interface *interface-name* at *time*

Description IGMP subscriber leave or timeout event.

NOTE: The *destination address* field for RPD_IGMP_LEAVE is no longer valid. To remove any processing impact relating to this message, the string "(null)" has been substituted for the destination address.

See the RPD_IGMP_ALL_SUBSCRIBERS_DELETED message for an interface down event.

Type Event: This message reports an event, not an error

Severity info

RPD_IGMP_MEMBERSHIP_TIMEOUT

System Log Message Membership timeout for listener *source-address* for group *group-address* source *sender-address* on interface *interface-name* at *time*

Description IGMP group membership timeout.

Type Event: This message reports an event, not an error

Severity info

RPD_ISIS_ADJDOWN

System Log Message IS-IS lost L*isis-level* adjacency to *neighbor-system-id*s on *interface-name*, reason: *reason*

Description An IS-IS adjacency with the indicated neighboring router was terminated. The local router no longer exchanges routing information with, or directs traffic to, the neighboring router.

Type Event: This message reports an event, not an error

Severity notice

Cause The communication path to the neighboring router was disrupted, a protocol error occurred, or the neighboring router was powered down.

RPD_ISIS_ADJUP

System Log Message IS-IS new L*isis-level* adjacency to *neighbor-system-id*s on *interface-name*

Description An IS-IS adjacency was established with the indicated neighboring router. The local router can now exchange information with it.

Type Event: This message reports an event, not an error

Severity info

RPD_ISIS_ADJUPNOIP

System Log Message IS-IS new L*isis-level* adjacency to *neighbor-system-id*s on *interface-name* without an address

Description An IS-IS adjacency was established with the indicated neighboring router, which is not configured for IS-IS for IP.

Type Event: This message reports an event, not an error

Severity notice

Cause The neighboring router is misconfigured: it is enabled for IS-IS but not for exchange of IP route information.

Action Configure the neighboring router for IS-IS with IP, or remove it from the IS-IS mesh.

RPD_ISIS_LDP_SYNC

System Log Message IS-IS interface *interface-name* advertised with infinite metric for *duration* seconds already due to loss of synchronization with LDP

Description The IS-IS protocol lost synchronization with the Label Distribution Protocol (LDP) on the indicated interface. As a consequence, it began advertising an infinite metric for the interface and has been doing so for the indicated number of seconds.

Type Error: An error occurred

Severity warning

Action Determine why LDP lost synchronization with IS-IS.

RPD_ISIS_LSPCKSUM

System Log Message IS-IS L*isis-level* LSP checksum error, interface *interface-name*, LSP id *lsp*l, sequence *sequence-number*, checksum *checksum*, lifetime *duration*

Description The indicated IS-IS informational link-state PDU (LSP) failed an internal checksum validity test, implying that it was corrupted.

Type Error: An error occurred

Severity warning

Cause The packet was corrupted in transit between the neighboring IS-IS router and this router, or memory on one of the routers was corrupted.

Action None, unless a large number of these messages appear in the system log file. The corrupted LSP is silently discarded.

RPD_ISIS_NO_ROUTERID

System Log Message IS-IS instance does not have a valid router ID

Description The IS-IS instance did not have a valid router ID.

Type Error: An error occurred

Severity alert

Cause When a router ID is not explicitly configured for an instance, IPv4 addresses configured under the instance are considered in the selection of the router ID. In this case, the instance did not have a router ID configured and no IPv4 addresses were configured.

Action Either configure a router ID by including the 'routing-instance' statement under the instance, or configure an IPv4 address by including the 'family inet' statement under one of the interfaces of the instance. You can also configure both.

RPD_ISIS_OVERLOAD

System Log Message IS-IS database overload

Description The IS-IS link-state database is full and no additional memory can be allocated for it.

Type Error: An error occurred

Severity alert

Cause No additional memory is available for storing IS-IS link-state information. Either system resources are exhausted or a software error occurred (such as a memory leak in the routing protocol process [rpd]). In the former case, IS-IS might be carrying too much information, or the router configuration includes too many features that use large amounts of system memory.

Action Perform one or more of the following actions: (1) Check for unusually high memory usage by the IS-IS task or rpd, (2) Unconfigure features that use large amounts of memory, (3) Add more memory to the Routing Engine, (4) Carry fewer IS-IS routes.

RPD_KRT_CCC_IFL_MODIFY

System Log Message *error-code*, *error-message*

Description The routing protocol process (rpd) attempted to modify the state for a logical interface that is related to circuit cross-connect (CCC), but the request failed.

Type Event: This message reports an event, not an error

Severity info

Cause It is possible that the kernel lacked the resources to fulfill the request. The rpd process will recover.

RPD_KRT_DELETED_RTT

System Log Message *task-name*: received deleted routing table from the kernel for family *address-family-type* table ID *table-id*

Description The routing protocol process (rpd) received a message from the kernel that referred to a routing table that no longer exists.

Type Error: An error occurred

Severity error

RPD_KRT_IFA_GENERATION

System Log Message ifa generation mismatch -- rpd *rpd-generation* kernel *kernel-generation*

Description The routing protocol process (rpd) received a message from the kernel in which the interface address associated with the indicated numerical index differed from the address-to-index mapping maintained by rpd.

Type Event: This message reports an event, not an error

Severity notice

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_KRT_IFDCHANGE

System Log Message *task-name* CHANGE for ifd *interface-device-index address/prefix-length* failed, error "*error-message*"

Description The routing protocol process (rpd) sent a request to the kernel to change the state of the indicated interface. The request failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request. The rpd process will recover.

RPD_KRT_IFDEST_GET

System Log Message *task-name* IFDEST GET for ifd *rpd-interface-name* failed, error "*error-message*"

Description The routing protocol process (rpd) requested state information about the indicated interface from the kernel. The request failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request. The rpd process will recover.

RPD_KRT_IFDGET

System Log Message *task-name* GET index for ifd *interface-name* failed, error "*error-message*"

Description The routing protocol process (rpd) requested state information about the indicated interface from the kernel. The request failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request. The rpd process will recover.

RPD_KRT_IFD_CELL_RELAY_INV_MODE

System Log Message Invalid mode (*mode*) specified for interface device *interface-name*; defaulting to port mode

Description The routing protocol process (rpd) received a message from the kernel that specified the cell-relay encapsulation for the indicated physical interface, but the specified cell-relay mode (port, or trunk user-to-network interface [UNI], or trunk network-to-network interface [NNI]) was invalid.

Type Error: An error occurred

Severity notice

RPD_KRT_IFD_CELL_RELAY_NO_MODE

System Log Message No mode specified for interface device *interface-name*; defaulting to port mode

Description The routing protocol process (rpd) received a message from the kernel that specified the cell-relay encapsulation for the indicated physical interface, but not the cell-relay mode.

Type Error: An error occurred

Severity notice

RPD_KRT_IFD_GENERATION

System Log Message ifd *interface-device-index* generation mismatch -- rpd *rpd-generation* kernel *kernel-generation*

Description The routing protocol process (rpd) received a message from the kernel in which the physical interface associated with the indicated numerical index differed from the interface-to-index mapping maintained by rpd.

Type Event: This message reports an event, not an error

Severity notice

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_KRT_IFL_CELL_RELAY_INV_MODE

System Log Message Invalid mode (*mode*) specified for logical interface *interface-name*; defaulting to port mode

Description The routing protocol process (rpd) received a message from the kernel that specified the cell-relay encapsulation for the indicated logical interface, but the specified cell-relay mode (port, virtual-circuit, or virtual-path) was invalid.

Type Error: An error occurred

Severity notice

RPD_KRT_IFL_CELL_RELAY_NO_MODE

System Log Message No mode specified for logical interface *interface-name*; defaulting to port mode

Description The routing protocol process (rpd) received a message from the kernel that specified the cell-relay encapsulation for the indicated logical interface but not the cell-relay mode.

Type Error: An error occurred

Severity notice

RPD_KRT_IFL_GENERATION

System Log Message ifl *logical-interface-index* generation mismatch -- rpd *rpd-interface-name rpd-generation* kernel *kernel-interface-name.kernel-interface-unit kernel-generation*

Description The routing protocol process (rpd) received a message from the kernel in which the logical interface associated with the indicated numerical index differed from the interface-to-index mapping maintained by rpd.

Type Event: This message reports an event, not an error

Severity notice

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_KRT_KERNEL_BAD_ROUTE

System Log Message *task-name*: lost *interface-hierarchy logical-interface-index* for route *route-prefix*

Description As it restarted, the routing protocol process (rpd) could not process a route obtained from the kernel because the route contained references to objects that are no longer valid.

Type Event: This message reports an event, not an error

Severity warning

Cause rpd did not recognize some elements in the route message, such as the logical interface index or an address family.

Action rpd can probably solve the problem, but check the entry for the indicated route prefix in the forwarding table. If the prefix's route and forwarding table entry are inconsistent, contact a technical support representative for instructions.

RPD_KRT_NEXTHOP_OVERFLOW

System Log Message *type route-prefix*: number of next hops (*count*) exceeded the maximum allowed (*maximum-value*) -- truncating

Description The number of next hops for the indicated route exceeded the indicated limit for a single route add operation.

Type Error: An error occurred

Severity error

Cause An indexed next hop can use multiple forwarding next hops per forwarding class. It is possible to have more next hops per route than can be carried in a single message. This requires that next hops be reused across forwarding classes, which is not recommended.

Action Eliminate common next hops across forwarding classes, thereby reducing the total number of next hops that must be specified.

RPD_KRT_NOIFD

System Log Message No device *interface-device-index* for interface *logical-interface-index* (*interface-name*)

Description The routing protocol process (rpd) received a message from the kernel that associated the indicated physical interface device and logical interface. The rpd process has no record of the device.

Type Error: An error occurred

Severity error

Cause It is possible that rpd discarded some interface messages from the kernel without processing them because it received more messages than it could handle. It will recover.

RPD_KRT_VERSION

System Log Message Routing socket version mismatch (kernel *kernel-version* != rpd *rpd-version*) -- kernel upgrade required

Description The routing protocol process (rpd) discovered that the kernel does not support the version of routing sockets it requires.

Type Error: An error occurred

Severity error

Cause The kernel version is older than the rpd version.

Action Upgrade the kernel package.

RPD_KRT_VERSIONNONE

System Log Message Routing socket message type *message-type*'s version is not supported by kernel, expected *rpd-version* -- kernel upgrade required

Description The routing protocol process (rpd) discovered that the kernel does not support the routing socket message types that it requires.

Type Error: An error occurred

Severity error

Cause The kernel version is older than the rpd version.

Action Upgrade the kernel package.

RPD_KRT_VERSIONOLD

System Log Message Routing socket message type *message-type*'s version is older than expected (*kernel-version* < *rpd-version*) -- consider upgrading the kernel

Description The routing protocol process (rpd) discovered that the kernel uses an older version of routing socket message types than it does.

Type Error: An error occurred

Severity error

Cause The kernel version is older than the rpd version.

Action Upgrade the kernel package.

RPD_KRT_VPLS_IFL_MODIFY

System Log Message Unable to modify VPLS-related state: *error-code* (errno *error-message*)

Description The routing protocol process (rpd) attempted to modify the state for a logical interface that is related to virtual private LAN service (VPLS), but the request failed.

Type Event: This message reports an event, not an error

Severity info

Cause It is possible that the kernel lacked the resources to fulfill the request. The rpd process will recover.

RPD_L2VPN_LABEL_ALLOC_FAILED

System Log Message Unable to allocate *label-type* labels for site *name* with ID *identifier* in instance *vpn-name*

Description The routing protocol process (rpd) could not allocate labels of the indicated type for the indicated site (name and ID) in the indicated virtual private network (VPN) virtual circuit (VC), because the resulting number of labels would have exceeded the limit.

Type Error: An error occurred

Severity error

RPD_L2VPN_REMOTE_SITE_COLLISION

System Log Message Two remote PEs (RDs *route-discriminator* and *route-discriminator2*) have the same site ID (*identifier*) in VPN *vpn-name*

Description The routing protocol process (rpd) for the indicated virtual private network (VPN) received an advertisement from a remote provider edge (PE) router with the first indicated route discriminator, but the associated site ID also belongs to a remote site with the second route discriminator.

Type Event: This message reports an event, not an error

Severity warning

RPD_L2VPN_SITE_COLLISION

System Log Message Same site ID *identifier* configured on remote PE (RD *route-discriminator*) and local PE in VPN *vpn-name* (non-multihomed site *name*)

Description The routing protocol process (rpd) for the indicated virtual private network (VPN) received an advertisement from a remote provider edge (PE) router, but the associated site ID belongs to a local site.

Type Event: This message reports an event, not an error

Severity error

RPD_LAYER2_VC_DOWN

System Log Message State of Layer 2 VC *vc-name* changed from UP to *state*

Description The state of the indicated Layer 2 virtual private network (VPN) virtual circuit (VC) changed as indicated (to either down or deleted).

Type Event: This message reports an event, not an error

Severity notice

RPD_LAYER2_VC_UP

System Log Message State of Layer 2 VC *vc-name* changed to UP

Description The state of the indicated Layer 2 virtual private network (VPN) virtual circuit (VC) changed to up.

Type Event: This message reports an event, not an error

Severity info

RPD_LDP_BFD_DOWN

System Log Message LDP BFD session for FEC *fec-address* went down

Description The routing protocol process (rpd) determined that the Label Distribution Protocol (LDP) Bidirectional Forwarding Detection (BFD) protocol session for the indicated forwarding equivalence class (FEC) terminated.

Type Event: This message reports an event, not an error

Severity notice

RPD_LDP_BFD_DOWN_TRACEROUTE_FAIL

System Log Message LDP BFD sessions for FEC *fec-address* going down due to traceroute failure

Description The routing protocol process (rpd) determined that the Label Distribution Protocol (LDP) Bidirectional Forwarding Detection (BFD) protocol session for the indicated forwarding equivalence class (FEC) was terminated due to traceroute failure.

Type Event: This message reports an event, not an error

Severity notice

RPD_LDP_BFD_UP

System Log Message LDP BFD session for FEC *fec-address* came up

Description The routing protocol process (rpd) determined that the Label Distribution Protocol (LDP) Bidirectional Forwarding Detection (BFD) protocol session for the indicated forwarding equivalence class (FEC) came up.

Type Event: This message reports an event, not an error

Severity notice

RPD_LDP_INTF_BLOCKED

System Log Message Duplicate session ID detected from *neighbor-address*i, interface *interface-name*, blocking interface

Description Label Distribution Protocol (LDP) operations were blocked on the indicated interface because the same session ID was detected across multiple interfaces but per-interface transport addresses are in use.

Type Event: This message reports an event, not an error

Severity warning

RPD_LDP_INTF_UNBLOCKED

System Log Message LDP interface *interface-name* is now unblocked

Description The indicated interface returned to the normal Label Distribution Protocol (LDP) operational state. It was previously blocked because the routing protocol process (rpd) noticed that a duplicate session ID was being used.

Type Event: This message reports an event, not an error

Severity warning

RPD_LDP_NBRDOWN

System Log Message LDP neighbor *neighbor-address*i (*interface-name*) is down

Description A Label Distribution Protocol (LDP) adjacency was terminated because the indicated neighbor stopped communicating. If the adjacency was the only one with this neighbor, the routing protocol process (rpd) terminated the associated LDP session.

Type Event: This message reports an event, not an error

Severity notice

RPD_LDP_NBRUP

System Log Message LDP neighbor *neighbor-address*i (*interface-name*) is up

Description A Label Distribution Protocol (LDP) adjacency with the indicated neighbor became active. The routing protocol process (rpd) established an LDP session with the neighbor if one did not already exist.

Type Event: This message reports an event, not an error

Severity info

RPD_LDP_SESSIONDOWN

System Log Message LDP session *neighbor-address*i is down, reason: *reason*

Description The routing protocol process (rpd) terminated a Label Distribution Protocol (LDP) session with the indicated neighbor and deleted all labels exchanged during the session.

Type Event: This message reports an event, not an error

Severity notice

RPD_LDP_SESSIONUP

System Log Message LDP session *neighbor-address*i is up

Description The routing protocol process (rpd) established a Label Distribution Protocol (LDP) session with the indicated neighbor. The routers began exchanging labels.

Type Event: This message reports an event, not an error

Severity info

RPD_LMP_ALLOC_ACK

System Log Message Unknown context in ALLOC_ACK message

Description The routing protocol process (rpd) received a label allocation acknowledgment that contained invalid context.

Type Error: An error occurred

Severity error

RPD_LMP_ALLOC_REQUEST_TIMEOUT

System Log Message Allocation request timeout for context 0x*address*, client request ID 0x*request-id*

Description The label allocation request with the indicated client request ID and for the indicated context timed out before completion.

Type Event: This message reports an event, not an error

Severity error

RPD_LMP_CONTROL_CHANNEL

System Log Message *operation* operation failed: control channel *logical-interface-index* unknown

Description The routing protocol process (rpd) received a message that specified the indicated type of operation on the indicated control channel. The channel does not exist.

Type Error: An error occurred

Severity error

RPD_LMP_NO_CALLBACK

System Log Message No function callback for label removed event

Description The routing protocol process (rpd) could not notify a client that a label was removed, because there was no function callback for the removal event.

Type Error: An error occurred

Severity error

RPD_LMP_NO_MEMORY

System Log Message *function-name*: malloc() failed (*error-message*, errno *error-code*)

Description The routing protocol process (rpd) could not allocate memory.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

RPD_LMP_NO_PEER

System Log Message Peer *peer-id* not found for TE link *link-name* (index *link-id*)

Description The routing protocol process (rpd) could not locate the indicated peer while processing a TE LINK message for the traffic-engineering link with the indicated name and index.

Type Error: An error occurred

Severity error

RPD_LMP_PEER

System Log Message *operation* operation failed: peer *peer-name* (index *peer-id*) *reason*

Description The routing protocol process (rpd) could not perform the indicated operation for the peer with the indicated name and index, for the indicated reason.

Type Error: An error occurred

Severity error

RPD_LMP_PEER_IFL

System Log Message *operation* operation failed because *reason* for peer *peer-name* (index *peer-id*): *error-message* (errno *error-code*)

Description The routing protocol process (rpd) could not perform the indicated operation for the peer with the indicated name and index, for the indicated reason.

Type Error: An error occurred

Severity error

RPD_LMP_PEER_INDEX

System Log Message No more peer indexes

Description No more peer indexes were available for allocation.

Type Event: This message reports an event, not an error

Severity error

RPD_LMP_RESOURCE

System Log Message *operation* operation failed: resource *resource* (type *type*, index *index*) *reason*

Description The routing protocol process (rpd) could not perform the indicated operation for the resource with the indicated name, type, and index, for the indicated reason.

Type Error: An error occurred

Severity error

RPD_LMP_RESOURCE_NO_LINK

System Log Message TE link *link-id* not found for resource *resource* (type *type*, index *index*)

Description The routing protocol process (rpd) could not locate the indicated traffic-engineering link for the resource with the indicated name, type, and index.

Type Error: An error occurred

Severity error

RPD_LMP_SEND

System Log Message *function-name*: handling write exception (*error-message*, errno *error-code*)

Description The routing protocol process (rpd) could not send a message to the Label Management Protocol (LMP) process (lmpd).

Type Error: An error occurred

Severity error

RPD_LMP_SEND_ALLOCATION_MESSAGE

System Log Message Unable to send allocation message: *error-message* (*error-code*)

Description The routing protocol process (rpd) could not send an allocation message.

Type Error: An error occurred

Severity error

RPD_LMP_SYSFAIL

System Log Message Unable to start *type* timer

Description The routing protocol process (rpd) discovered that the Label Management Protocol (LMP) process (lmpd) was not running. The rpd process attempted to start the indicated type of timer for restarting the lmpd process or reestablishing a connection to it, but the attempt failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Examine the messages that immediately follow this message in the system log for information about possible reasons that lmpd failed.

RPD_LMP_TE_LINK

System Log Message *operation* operation failed: TE link *link-name* (index *index*) *reason*

Description The routing protocol process (rpd) could not perform the indicated operation for the traffic-engineering link with the indicated name and index, for the indicated reason.

Type Error: An error occurred

Severity error

RPD_LMP_TE_LINK_INDEX

System Log Message No more TE-link indexes

Description No more traffic-engineering link indexes were available for allocation.

Type Event: This message reports an event, not an error

Severity error

RPD_LMP_UNEXPECTED_OPCODE

System Log Message *message-type* message had unexpected operation code *operation-code*

Description The routing protocol process (rpd) received the indicated type of message, which had the indicated invalid operation code.

Type Error: An error occurred

Severity error

RPD_LOCK_FLOCKED

System Log Message Unable to obtain a lock on *filename*, is another copy of rpd running?

Description The routing protocol process (rpd) could not obtain the mutual exclusion lock that prevents more than one instance of rpd from running simultaneously. The system terminated the indicated process.

Type Error: An error occurred

Severity error

Cause Another rpd process is running.

Action Use the 'show system process' command to verify that another rpd is running.

RPD_LOCK_LOCKED

System Log Message Unable to obtain a lock on *filename*, *program-name*[*pid*] is still running

Description The routing protocol process (rpd) could not obtain the mutual exclusion lock that prevents more than one instance of rpd from running simultaneously. The system terminated this instance of rpd.

Type Error: An error occurred

Severity error

Cause Another rpd is running.

Action Use the 'show system process' command to verify that another rpd is running.

RPD_MC_DESIGNATED_PE_CHANGE

System Log Message Designated forwarder changed to *ip-address* for backup-pe-group *group-name* in *routing-instance* instance

Description The routing protocol daemon (rpd) assigned the indicated Provider Edge (PE) as the new designated forwarder of the indicated routing instance for the indicated backup-pe-group.

Type Event: This message reports an event, not an error

Severity notice

RPD_MC_LOCAL_DESIGNATED_PE

System Log Message Local PE is now the designated forwarder for backup-pe-group *group-name* in *routing-instance* instance

Description The routing protocol daemon (rpd) selected the local Provider Edge (PE) as the designated forwarder of the indicated routing instance for the indicated backup-pe-group.

Type Event: This message reports an event, not an error

Severity notice

RPD_MC_OIF_REJECT

System Log Message Interface *interface-name* is rejected due to lack of bw

Description When multicast bandwidth admission control is applied, an interface may not be put into the downstream interface list for a forwarding cache if the interface does

not have enough bandwidth for the flow, even when a multicast protocol determines that there are local/downstream receivers.

Type Event: This message reports an event, not an error

Severity info

RPD_MC_OIF_RE_ADMIT

System Log Message Interface *interface-name* is re-admitted with newly available bw

Description The indicated downstream interface that was previously rejected was readmitted for the flow because there was newly availabe bandwidth on the interface.

Type Event: This message reports an event, not an error

Severity info

RPD_MGMT_TIMEOUT

System Log Message Connection to management peer *process-name* timed out waiting for input

Description The connection between the routing protocol process (rpd) and the indicated management process (mgd) timed out before input arrived from the mgd process.

Type Error: An error occurred

Severity warning

RPD_MIRROR_ERROR

System Log Message Unable to establish mirror connection between Routing Engines: *error-message*

Description The routing protocol process (rpd) could not establish the mirror connection (which supports nonstop routing) between the master and backup Routing Engines.

Type Error: An error occurred

Severity warning

Cause The master and backup Routing Engines are running incompatible versions of the JUNOS software.

Action Update the JUNOS software to compatible versions on the master and backup Routing Engines.

RPD_MIRROR_VERSION_MISMATCH

System Log Message Versions of mirror software on Routing Engines are incompatible: *error-message*

Description While trying to establish the mirror connection between the master and backup Routing Engines (which supports nonstop routing), the routing protocol process (rpd) determined that the versions of JUNOS software on the Routing Engines were incompatible.

Type Error: An error occurred

Severity warning

Action Update the JUNOS software to compatible versions on the master and backup Routing Engines.

RPD_MLD_ACCOUNTING_OFF

System Log Message *interface-name time*

Description The Multicast Listener Discovery (MLD) accounting for the indicated interface was disabled at the indicated time.

Type Event: This message reports an event, not an error

Severity info

RPD_MLD_ACCOUNTING_ON

System Log Message *interface-name time*

Description The Multicast Listener Discovery (MLD) accounting for the indicated interface was enabled at the indicated time.

Type Event: This message reports an event, not an error

Severity info

RPD_MLD_ALL_SUBSCRIBERS_DELETED

System Log Message All subscribers on interface *interface-name* deleted at *time* because the interface is down

Description MLD interface down event.

Type Event: This message reports an event, not an error

Severity info

RPD_MLD_CFG_CREATE_ENTRY_FAILED

System Log Message Could not create entry for *entry*.

Description MLD failed to create the indicated configuration entry. The configuration request failed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_MLD_CFG_INVALID_VALUE

System Log Message The *object-name* configuration object *identifier* field has an invalid value of *value*

Description The configuration request failed because the indicated configuration object contained the indicated invalid value.

Type Error: An error occurred

Severity error

Action Modify configuration statement to use a valid value.

RPD_MLD_DYN_CFG_INVALID_STMT

System Log Message Invalid dynamic configuration statement: *configuration-statement*

Description The indicated dynamic configuration statement was invalid. The dynamic configuration instantiation request was rejected.

Type Error: An error occurred

Severity error

Action Remove the unsupported configuration statement.

RPD_MLD_DYN_CFG_SES_ID_MISMATCH

System Log Message Dynamic configuration entry for interface *interface-name* with session id *client-session-id* found an existing entry with a different session id of *client-session-id-1*.

Description The dynamic configuration instantiation request matched an existing dynamic configuration block that had a different session id. The dynamic configuration instantiation request was rejected.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_MLD_JOIN

System Log Message Listener *source-address* sent a join to *destination-address* for group *group-address* source *sender-address* on interface *interface-name* at *time*

Description MLD join event.

NOTE: The *destination address* field for RPD_MLD_JOIN is no longer valid. To remove any processing impact relating to this message, the string “(null)” has been substituted for the destination address.

Type Event: This message reports an event, not an error

Severity info

RPD_MLD_LEAVE

System Log Message Listener *source-address* sent a leave to *destination-address* for group *group-address* source *sender-address* on interface *interface-name* at *time*

Description MLD subscriber leave or timeout event.

NOTE: The *destination address* field for RPD_MLD_LEAVE is no longer valid. To remove any processing impact relating to this message, the string “(null)” has been substituted for the destination address.

See the RPD_MLD_ALL_SUBSCRIBERS_DELETED message for an interface down event.

Type Event: This message reports an event, not an error

Severity info

RPD_MLD_MEMBERSHIP_TIMEOUT

System Log Message Membership timeout for listener *source-address* for group *group-address* source *sender-address* on interface *interface-name* at *time*

Description MLD group membership timeout.

Type Event: This message reports an event, not an error

Severity info

RPD_MPLS_LSP_BANDWIDTH_CHANGE

System Log Message MPLS LSP *lsp-name* bandwidth changed, lsp bandwidth *bandwidth* bps

Description The bandwidth associated with the indicated Multiprotocol Label Switching (MPLS) label-switched path (LSP) changed.

Type Event: This message reports an event, not an error

Severity warning

RPD_MPLS_LSP_CHANGE

System Log Message MPLS LSP *lsp-name* change on *path-type*(*pathname*) Route *lsp-rro* lsp bandwidth *bandwidth* bps

Description The indicated Multiprotocol Label Switching (MPLS) label-switched path (LSP) was rerouted and its Record Route Object (RRO) changed.

Type Event: This message reports an event, not an error

Severity warning

RPD_MPLS_LSP_DOWN

System Log Message MPLS LSP *lsp-name* down on *path-type*(*pathname*)

Description The indicated Multiprotocol Label Switching (MPLS) label-switched path (LSP) went down and could not be used to send traffic.

Type Event: This message reports an event, not an error

Severity warning

RPD_MPLS_LSP_SWITCH

System Log Message MPLS LSP *lsp-name* switch from *old-path-type*(*old-pathname*) to *new-path-type*(*new-pathname*), Route *lsp-rro*: *reason* lsp bandwidth *bandwidth* bps

Description The indicated Multiprotocol Label Switching (MPLS) label-switched path (LSP) switched from primary path to secondary path or vice versa.

Type Event: This message reports an event, not an error

Severity warning

RPD_MPLS_LSP_UP

System Log Message MPLS LSP *lsp-name* up on *path-type*(*pathname*) Route *lsp-rro* lsp bandwidth *bandwidth* bps

Description The indicated Multiprotocol Label Switching (MPLS) label-switched path (LSP) came up and could be used to send traffic.

Type Event: This message reports an event, not an error

Severity warning

RPD_MPLS_OAM_READ_ERROR

System Log Message Unable to read from pipe to MPLS OAM process: *reason* (*error-message*)

Description The routing protocol process (rpd) could not read a message available on the read pipe from the MPLS Operation, Administration, and Maintenance process (mplsoamd).

Type Error: An error occurred

Severity info

Action Contact your technical support representative.

RPD_MPLS_OAM_WRITE_ERROR

System Log Message Unable to write to pipe to MPLS OAM process: (*error-message*)

Description The routing protocol process (rpd) could not write a message on the write pipe to the MPLS Operation, Administration, and Maintenance process (mplsoamd).

Type Error: An error occurred

Severity info

Action Contact your technical support representative.

RPD_MPLS_PATH_BANDWIDTH_CHANGE

System Log Message MPLS path *pathname* (lsp *lsp-name*) bandwidth changed, path bandwidth *bandwidth* bps

Description The bandwidth associated with the indicated Multiprotocol Label Switching (MPLS) path changed.

Type Event: This message reports an event, not an error

Severity warning

RPD_MPLS_PATH_BFD_DOWN

System Log Message BFD session for MPLS path *pathname* went down on LSP *lsp-name*

Description The routing protocol process (rpd) determined that the Bidirectional Forwarding Detection (BFD) protocol session for the indicated Multiprotocol Label Switching (MPLS) path terminated on the indicated label-switched path (LSP).

Type Event: This message reports an event, not an error

Severity notice

RPD_MPLS_PATH_BFD_UP

System Log Message BFD session for MPLS path *pathname* came up on LSP *lsp-name*

Description The routing protocol process (rpd) determined that the Bidirectional Forwarding Detection (BFD) protocol session for the the indicated Multiprotocol Label Switching (MPLS) path came up on the indicated label-switched path (LSP).

Type Event: This message reports an event, not an error

Severity notice

RPD_MPLS_PATH_BW_NOT_AVAILABLE

System Log Message Unable to satisfy bandwidth configured for MPLS path *pathname* on LSP *lsp-name*

Description The bandwidth setting for the indicated Multiprotocol Label Switching (MPLS) path and label-switched path (LSP) was changed recently, but attempts to apply the new setting failed. The LSP continued to use the previous amount of bandwidth.

Type Event: This message reports an event, not an error

Severity warning

Action Determine the reason that the bandwidth could not change and make the necessary changes to the software configuration, hardware configuration, or both.

RPD_MPLS_PATH_DOWN

System Log Message MPLS path *pathname* down on LSP *lsp-name*

Description The indicated Multiprotocol Label Switching (MPLS) path went down on the indicated label-switched path (LSP).

Type Event: This message reports an event, not an error

Severity warning

RPD_MPLS_PATH_UP

System Log Message MPLS path *pathname* up on LSP *lsp-name* path bandwidth *bandwidth* bps

Description The indicated Multiprotocol Label Switching (MPLS) path came up on the indicated label-switched path (LSP).

Type Event: This message reports an event, not an error

Severity warning

RPD_MSDP_PEER_DOWN

System Log Message MSDP peer *peer-address* peer-group *peer-group* out of Established state

Description The indicated MSDP peer left the Established state. The routing protocol process (rpd) deleted all active sources learned from the peer and will no longer send 'Source Active' messages to it.

Type Event: This message reports an event, not an error

Severity notice

RPD_MSDP_PEER_UP

System Log Message MSDP peer *peer-address* peer-group *peer-group* into Established state

Description The indicated MSDP peer entered the Established state.

Type Event: This message reports an event, not an error

Severity info

RPD_MSDP_SRC_ACTIVE_OVER_LIMIT

System Log Message Number of MSDP source-active messages about *originator* exceeded configured limit *message*

Description The number of MSDP source-active messages received from the indicated instance, peer, or source exceeded the configured limit. All source-active messages are discarded until the limit is no longer exceeded. During periods when the event reported by this message occurs frequently, the routing protocol process (rpd) does not log every occurrence. In this case, the repetitions field in the message indicates how many times the event occurred since the rpd process previously logged this message.

Type Event: This message reports an event, not an error

Severity notice

RPD_MSDP_SRC_ACTIVE_OVER_THRESH

System Log Message Number of MSDP source-active messages about *originator* exceeded configured threshold *message*

Description The number of MSDP source-active messages received from the indicated instance, peer, or source exceeded the configured threshold. Until the threshold is no longer

exceeded, a random early discard (RED) profile is applied to incoming messages so that only some of them are accepted. During periods when the event reported by this message occurs frequently, the routing protocol process (rpd) does not log every occurrence. In this case, the repetitions field in the message indicates how many times the event occurred since the rpd process previously logged this message.

Type Event: This message reports an event, not an error

Severity notice

RPD_MSDP_SRC_ACTIVE_UNDER_LIMIT

System Log Message Number of MSDP source-active messages about *originator* no longer exceeded configured limit *message*

Description The number of MSDP source-active messages received from the indicated instance, peer, or source no longer exceeded the configured limit. Active-source messages are no longer discarded automatically. During periods when the event reported by this message occurs frequently, the routing protocol process (rpd) does not log every occurrence. In this case, the repetitions field in the message indicates how many times the event occurred since the rpd process previously logged this message.

Type Event: This message reports an event, not an error

Severity notice

RPD_MSDP_SRC_ACTIVE_UNDER_THRESH

System Log Message Number of MSDP source-active messages about *originator* no longer exceeded configured threshold *message*

Description The number of MSDP source-active messages received from the indicated instance, peer, or source no longer exceeded the configured threshold. A random early discard (RED) profile is no longer applied to incoming messages. During periods when the event reported by this message occurs frequently, the routing protocol process (rpd) does not log every occurrence. In this case, the repetitions field in the message indicates how many times the event occurred since the rpd process previously logged this message.

Type Event: This message reports an event, not an error

Severity notice

RPD_OSPF_CFGNBR_P2P

System Log Message Ignored configured neighbors on point-to-point realm *realm-name* interface *interface-name* area *area-id*i

Description For point-to-point interfaces, OSPF neighbors are learned by using hello messages, so the implicit configuration of neighbors was ignored for the indicated point-to-point interface.

Type Error: An error occurred

Severity warning

Action Remove the neighbor configuration for the indicated interface.

RPD_OSPF_LDP_SYNC

System Log Message OSPF realm *realm-name* interface *interface-name* area *area-id*i advertised with infinite metric for *duration* seconds already due to loss of synchronization with LDP

Description The OSPF protocol lost synchronization with the Label Distribution Protocol (LDP) on the indicated interface. As a consequence, it began advertising an infinite metric for the interface and has been doing so for the indicated number of seconds.

Type Error: An error occurred

Severity warning

Action Determine why LDP lost synchronization with OSPF.

RPD_OSPF_NBRDOWN

System Log Message OSPF neighbor *neighbor-address* (realm *realm-name interface-name* area *area-id*i) state changed from *old-state* to *new-state* due to *event-name* (event reason: *reason*)

Description An OSPF adjacency with the indicated neighboring router was terminated. The local router no longer exchanges routing information with, or directs traffic to, the neighboring router.

Type Event: This message reports an event, not an error

Severity notice

RPD_OSPF_NBRUP

System Log Message OSPF neighbor *neighbor-address* (realm *realm-name interface-name* area *area-id*i) state changed from *old-state* to *new-state* due to *event-name* (event reason: *reason*)

Description An OSPF adjacency was established with the indicated neighboring router. The local router can now exchange information with it.

Type Event: This message reports an event, not an error

Severity info

RPD_OSPF_OVERLOAD

System Log Message OSPF instance *instance* topology *topology* is going into overload state: number of export prefixes (*count*) exceeded maximum allowed (*maximum-value*)

Description The indicated topology in the indicated OSPF instance became overloaded and will remain in that state until an administrator intervenes.

Type Error: An error occurred

Severity warning

Cause The number of export prefixes exceeded the configured limit.

Action Unconfigure or modify export policies that inject a large number of routes.

RPD_OS_MEMHIGH

System Log Message Using *size* KB of memory, *percentage-value* percent of available

Description The routing protocol process (rpd) is using the indicated amount and percentage of Routing Engine memory, which is considered excessive.

Type Error: An error occurred

Severity error

Cause Either rpd is leaking memory or the use of system resources is excessive, perhaps because routing filters are misconfigured or the configured network topology is very complex.

Action Increase the amount of RAM in the Routing Engine.

RPD_PARSE_BAD_LR_NAME

System Log Message *executable-name*: logical router name "*logical-router-name*"exceeds *count* characters

Description The indicated logical router name exceeds the indicated maximum number of characters.

Type Error: An error occurred

Severity error

Action Assign a shorter name.

RPD_PARSE_BAD_OPTION

System Log Message *executable-name*: command-line option *option* is invalid

Description The command line used to start the indicated process included the indicated option, which is invalid. The process did not start.

Type Error: An error occurred

Severity error

Action Reissue the command without the invalid option.

RPD_PARSE_CMD_ARG

System Log Message *executable-name*: missing required argument for command-line option *option*

Description The command line used to start the indicated process did not include the argument required by the indicated option. The process did not start.

Type Error: An error occurred

Severity error

Action Reissue the command and include the required argument.

RPD_PARSE_CMD_DUPLICATE

System Log Message *executable-name*: command-line option *option* is a duplicate

Description The command line used to start the indicated process included the indicated duplicate option. The process did not start.

Type Error: An error occurred

Severity error

Action Reissue the command without the duplicate option.

RPD_PARSE_CMD_EXTRA

System Log Message *executable-name*: command-line option *option* is extraneous

Description The command line used to start the indicated process included the indicated option, which is extraneous. The process did not start.

Type Error: An error occurred

Severity error

Action Reissue the command and omit the extraneous option.

RPD_PIM_NBRDOWN

System Log Message PIM neighbor *neighbor-address* (*interface-name*) removed due to: *reason*

Description The routing protocol process (rpd) declared the indicated PIM neighbor inactive.

Type Event: This message reports an event, not an error

Severity notice

RPD_PIM_NBRUP

System Log Message PIM new neighbor *neighbor-address* interface *interface-name*

Description The routing protocol process (rpd) discovered the indicated new PIM neighbor on the indicated interface.

Type Event: This message reports an event, not an error

Severity info

RPD_PPM_READ_ERROR

System Log Message Read error on pipe from ppmd: *reason* (*error-message*)

Description The routing protocol process (rpd) could not read a message available on the read pipe from the periodic packet management process (ppmd).

Type Error: An error occurred

Severity info

Action Contact your technical support representative.

RPD_PPM_WRITE_ERROR

System Log Message *function-name*: write error on pipe to ppmd (*error-message*)

Description The routing protocol process (rpd) could not write a message on the pipe to the periodic packet management process (ppmd).

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_RDISC_CKSUM

System Log Message Bad checksum for router solicitation from *source-address* to *destination-address*

Description The routing protocol process (rpd) ignored a router discovery solicitation message from the indicated address because the checksum in the message's ICMP header was invalid.

Type Event: This message reports an event, not an error

Severity warning

Cause The solicitation message was incorrectly generated or damaged in transit.

Action Examine the host that generated the solicitation message.

RPD_RDISC_NOMULTI

System Log Message Ignoring interface *interface-address* on *interface-name* -- multicast not available

Description The indicated interface was configured for router discovery, but does not support IP multicast operations as required. The routing protocol process (rpd) did not enable router discovery on the interface.

Type Error: An error occurred

Severity warning

Action Do not configure router discovery on the interface.

RPD_RDISC_NORECVIF

System Log Message Unable to locate interface for router solicitation from *source-address* to *destination-address*

Description The routing protocol process (rpd) ignored a router discovery solicitation message from the indicated router because the router's IP address does not share the IP prefix of the local router. The local router is not a candidate for the indicated router because they are not on the same network.

Type Event: This message reports an event, not an error

Severity warning

Cause Although the indicated router seems to be locally attached, no interfaces on the local router are configured to handle its IP address. Either the indicated router is configured with the wrong IP address, or the local router is not correctly configured for the network that the indicated router is using.

Action Ignore this message if it indicates the desired configuration, or reconfigure one or both routers to share a common network.

RPD_RDISC_SOLICITADDR

System Log Message Expected multicast (*expected-address*) for router solicitation from *source-address* to *destination-address*

Description A router discovery solicitation message received from the indicated address was not sent to the expected multicast address for all routers.

Type Event: This message reports an event, not an error

Severity warning

Action Examine the configuration of the router that generated the router discovery solicitation message.

RPD_RDISC_SOLICITICMP

System Log Message Nonzero ICMP code (*value*) for router solicitation from *source-address* to *destination-address*

Description The routing protocol process (rpd) ignored a router discovery solicitation message from the indicated router because the ICMP code in the message header was nonzero.

Type Event: This message reports an event, not an error

Severity warning

Cause The solicitation message was incorrectly generated.

Action Examine the host that generated the solicitation message.

RPD_RDISC_SOLICITLEN

System Log Message Insufficient length (*length*) for router solicitation from *source-address* to *destination-address*

Description The routing protocol process (rpd) ignored a router discovery solicitation message from the indicated router, because the indicated message length is too short.

Type Event: This message reports an event, not an error

Severity warning

Cause The solicitation message was incorrectly generated.

Action Examine the host that generated the solicitation message.

RPD_RIP_AUTH

System Log Message Update with invalid authentication from *source-address* (*interface-name*)

Description The routing protocol process (rpd) ignored a RIP update because authentication of the update failed.

Type Event: This message reports an event, not an error

Severity notice

RPD_RIP_JOIN_BROADCAST

System Log Message Unable to get broadcast address on *interface-name*; using the all-ones address

Description RIP cannot run on the indicated interface because the routing protocol process (rpd) could not obtain the broadcast address on the interface as required for running RIP version 1 or version 2 in compatibility mode.

Type Error: An error occurred

Severity error

RPD_RIP_JOIN_MULTICAST

System Log Message Unable to join multicast group on *interface-name*: *error-message*

Description RIP cannot run on the indicated interface, because the routing protocol process (rpd) could not join the RIP multicast group as required for RIP version 2 multicast updates.

Type Error: An error occurred

Severity error

RPD_RSVP_BACKUP_DOWN

System Log Message Backup for protecting LSP *lsp-name* down, using bypass *bypass-lsp-namereason*

Description When link protection is enabled, a backup label-switched path (LSP) is needed to maintain a protected LSP's control-plane connectivity when topology failures are detected. The backup LSP for the indicated protected LSP failed. The failure can cause traffic loss because the protected LSP tears down when there is no backup. If the reason for the backup failure can be determined, it is reported in the message.

Type Event: This message reports an event, not an error

Severity warning

RPD_RSVP_BYPASS_DOWN

System Log Message RSVP bypass *bypass-lsp-name* for protecting interface *interface-name* went down*reason*

Description The indicated RSVP link-protection bypass, which was protecting the indicated interface, was terminated. If the reason for the termination can be determined, it is reported in the message.

Type Event: This message reports an event, not an error

Severity warning

RPD_RSVP_BYPASS_UP

System Log Message RSVP bypass *bypass-lsp-name* for protecting interface *interface-name* came up

Description The indicated RSVP link-protection bypass was established to protect the indicated interface.

Type Event: This message reports an event, not an error

Severity warning

RPD_RSVP_LSP_SWITCH

System Log Message RSVP LSP *lsp-name* switched to backup; using bypass LSP *bypass-lsp-name*, route *lsp-rro*

Description RSVP detected a failure downstream for the indicated label-switched path (LSP) and switched it to a backup using the indicated bypass LSP.

Type Event: This message reports an event, not an error

Severity warning

Cause The downstream interface or router for the LSP went down.

RPD_RSVP_MAXIMUM_SESSIONS

System Log Message RSVP maximum session limit of *limit* reached

Description The routing protocol process (rpd) could not set up an RSVP session because the indicated limit on the number of sessions was reached.

Type Event: This message reports an event, not an error

Severity warning

RPD_RSVP_NBRDOWN

System Log Message RSVP neighbor *neighbor-address* down on interface *interface-name*, *reason*

Description The RSVP neighbor to the indicated address was terminated.

Type Event: This message reports an event, not an error

Severity warning

Cause The communication path to the neighboring router was disrupted, a protocol error occurred, or the neighboring router was powered down.

RPD_RSVP_NBRUP

System Log Message RSVP neighbor *neighbor-address* up on interface *interface-name*

Description An RSVP neighbor was established to the indicated address.

Type Event: This message reports an event, not an error

Severity warning

RPD_RT_CFG_CREATE_ENTRY_FAILED

System Log Message Could not create entry *entry*

Description RT failed to create the indicated configuration entry. The configuration request failed.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

RPD_RT_CFG_INVALID_VALUE

System Log Message The *object-name* configuration object *identifier* field has an invalid value of *value*

Description The configuration request failed because the indicated configuration object contained the indicated invalid value.

Type Error: An error occurred

Severity error

Action Modify configuration statement to use a valid value.

RPD_RT_DUPLICATE_RD

System Log Message routing-instance *routing-instance* has duplicate route-distinguisher *route-discriminator* as routing-instance *existing-routing-instance*

Description The route-distinguisher assigned to this routing instance has already been assigned to another routing instance (as indicated).

Type Error: An error occurred

Severity error

RPD_RT_ERROR

System Log Message rt_event_*event-name*: fatal state error

Description A route in the routing table was found to be in an unrecoverable error state.

Type Error: An error occurred

Severity critical

RPD_RT_IFUP

System Log Message UP route for interface *interface-name* index *logical-interface-index address/prefix-length*

Description The interface route for the indicated interface and prefix changed state from down to up, becoming available for routing.

Type Event: This message reports an event, not an error

Severity warning

RPD_RT_PATH_LIMIT_BELOW

System Log Message Number of paths (*count*) in table *table-name* is now less than the configured maximum (*limit*)

Description The number of paths in the indicated routing table previously equaled or exceeded the indicated limit, but went down to the indicated number, which is below the limit.

Type Event: This message reports an event, not an error

Severity warning

RPD_RT_PATH_LIMIT_REACHED

System Log Message Number of paths (*count*) in table *table-name status* configured maximum (*limit*)

Description The indicated total number of paths in the indicated routing table equaled or exceeded the indicated configured limit. Attempts to add some types of path to the table fail while this condition holds, but the path count can exceed the limit if paths are forcibly added (for example, for static routes). This message first appears in the log when the limit is reached and repeats periodically until the number of paths goes below the limit.

Type Error: An error occurred

Severity error

RPD_RT_PATH_LIMIT_WARNING

System Log Message Number of paths (*count*) in table *table-name* reached warning threshold (*threshold* percent of configured maximum *limit*)

Description The indicated total number of paths in the indicated routing table reached the threshold for a warning. The threshold is the indicated percentage of the indicated configured limit on the number of paths.

Type Event: This message reports an event, not an error

Severity warning

RPD_RT_PREFIX_LIMIT_BELOW

System Log Message Number of prefixes (*prefix-count*) in table *table-name* is now less than the configured maximum (*limit*)

Description The number of prefixes in the indicated routing table previously equaled or exceeded the indicated limit, but went down to the indicated number, which is below the limit.

Type Event: This message reports an event, not an error

Severity warning

RPD_RT_PREFIX_LIMIT_REACHED

System Log Message Number of prefixes (*prefix-count*) in table *table-name status* configured maximum (*limit*)

Description The indicated total number of prefixes in the indicated routing table equaled or exceeded the indicated configured limit. Attempts to add some types of prefix to the table fail while this condition holds, but the prefix count can exceed the limit if prefixes are forcibly added (for example, for static routes). This message first appears in the log when the limit is reached and repeats periodically until the number of prefixes goes below the limit.

Type Error: An error occurred

Severity error

RPD_RT_PREFIX_LIMIT_WARNING

System Log Message Number of prefixes (*prefix-count*) in table *table-name* reached warning threshold (*threshold* percent of configured maximum *limit*)

Description The indicated total number of prefixes in the indicated routing table reached the threshold for a warning. The threshold is the indicated percentage of the indicated configured limit on the number of prefixes.

Type Event: This message reports an event, not an error

Severity warning

RPD_RT_SHOWMODE

System Log Message invalid display mode (*mode*)

Description The indicated display mode was specified in a 'show route' command and is unsupported.

Type Error: An error occurred

Severity error

RPD_RT_TAG_ID_ALLOC_FAILED

System Log Message Unable to allocate *object-name* for routing instance *instance*

Description The routing protocol process (rpd) could not allocate either labels or subunits (as indicated) for the indicated routing instance, because the result number of objects would have exceeded the limit.

Type Error: An error occurred

Severity error

RPD_SCHED_CALLBACK_LONGRUNTIME

System Log Message *function-name*: excessive runtime *time* during *action* of *module*

Description The indicated submodule of the routing protocol process (rpd) ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

RPD_SCHED_CUMULATIVE_LONGRUNTIME

System Log Message *function-name*: excessive runtime (total of *time* in *count* callbacks) after *action* of *module*

Description Several submodules of the routing protocol process (rpd) ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

RPD_SCHED_MODULE_LONGRUNTIME

System Log Message *function-name*: excessive runtime *time* during *action* of *module*

Description Several submodules of the routing protocol process (rpd) ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

RPD_SCHED_TASK_LONGRUNTIME

System Log Message *function-name* ran for *total-time* (*user-time* user, *system-time* system) doing *action*

Description A task callback within the routing protocol process (rpd) ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

RPD_SIGNAL_TERMINATE

System Log Message *signal-name* termination signal received

Description In response to the indicated termination request, the routing protocol process (rpd) terminated adjacencies with neighbors and shut down.

Type Event: This message reports an event, not an error

Severity notice

RPD_SNMP_CONN_PROG

System Log Message *function-name*: *error-message*

Description The indicated error occurred while the routing protocol process (rpd) was connecting to the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity info

RPD_SNMP_CONN_QUIT

System Log Message *function-name*: unable to connect to SNMP agent (*pathname*): *error-message*

Description The routing protocol process (rpd) could not connect to the indicated Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

RPD_SNMP_CONN_RETRY

System Log Message *function-name*: reattempting connection to SNMP agent (*pathname*): *error-message*

Description The routing protocol process (rpd) tried again to connect to the indicated Simple Network Management Protocol (SNMP) master agent after a connection attempt failed.

Type Error: An error occurred

Severity error

RPD_SNMP_INVALID_SOCKET

System Log Message *function-name*: socket *file-descriptor* is invalid

Description The routing protocol process (rpd) could not send a message to a Simple Network Management Protocol (SNMP) master agent because the indicated socket is invalid.

Type Error: An error occurred

Severity error

RPD_SNMP_SOCKOPT_BLOCK

System Log Message *function-name*: unable to set nonblocking option

Description The routing protocol process (rpd) could not set a socket to nonblocking mode after connecting to the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

RPD_SNMP_SOCKOPT_RECVBUF

System Log Message *function-name*: unable to set recvbuf option

Description The routing protocol process (rpd) could not set the size of the kernel receive buffer, which allows it to accept the largest possible packet from the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

RPD_SNMP_SOCKOPT_SENDBUF

System Log Message *function-name*: unable to set sendbf option

Description The routing protocol process (rpd) could not set the size of the kernel send buffer, which allows it to send the largest possible packet to the Simple Network Management Protocol (SNMP) master agent.

Type Error: An error occurred

Severity error

RPD_START

System Log Message Start *executable-name*[*pid*] version *version* built *date*

Description The routing protocol process (rpd) started.

Type Event: This message reports an event, not an error

Severity info

RPD_SYSTEM

System Log Message *reason*: *error-message*

Description A system call made by the routing protocol process (rpd) failed.

Type Error: An error occurred

Severity info

Cause It is possible that the kernel lacked the resources to fulfill the request. The rpd process will recover.

RPD_TASK_BEGIN

System Log Message Commencing routing updates, version *rpd-version*, built *date* by *builder*

Description The routing protocol process (rpd) started.

Type Event: This message reports an event, not an error

Severity notice

RPD_TASK_CHILDKILLED

System Log Message *task-name* terminated by SIG*signal-namecore-dump-status*

Description While a child process of the routing protocol process (rpd) was performing the indicated operation, it terminated in response to the indicated signal.

Type Event: This message reports an event, not an error

Severity error

RPD_TASK_CHILDSTOPPED

System Log Message *task-name* stopped by SIG*signal-name*

Description While a child process of the routing protocol process (rpd) was performing the indicated operation, it stopped in response to the indicated signal.

Type Event: This message reports an event, not an error

Severity error

RPD_TASK_FORK

System Log Message Unable to fork *task-name*: *error-message*

Description The routing protocol process failed to create the indicated child process.

Type Error: An error occurred

Severity error

RPD_TASK_GETWD

System Log Message getwd: *error-message*

Description The getwd() system call made by the routing protocol process (rpd) failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request. The rpd process will recover.

RPD_TASK_MASTERSHIP

System Log Message Assuming mastership

Description The routing protocol process (rpd) became active when the Routing Engine on which it was running assumed mastership.

Type Event: This message reports an event, not an error

Severity info

RPD_TASK_NOREINIT

System Log Message Reinitialization not possible

Description The routing protocol process (rpd) failed to reinitialize as requested, because it was running in a state that did not allow reconfiguration.

Type Error: An error occurred

Severity error

RPD_TASK_PIDCLOSED

System Log Message Unable to close and remove *filename*: *error-message*

Description The routing protocol process (rpd) tried to close and remove the file that records its process ID (PID), which serves to prevent multiple instances of rpd from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

RPD_TASK_PIDFLOCK

System Log Message flock(*filename*, LOCK_EX): *error-message*

Description The routing protocol process (rpd) issued the flock() system call on the file that records its process ID (PID), which serves to prevent multiple instances of rpd from running simultaneously. The system call failed.

Type Error: An error occurred

Severity error

RPD_TASK_PIDWRITE

System Log Message Unable to write to fd *filename*: *error-message*

Description The routing protocol process (rpd) tried to write to the file that records its process ID (PID), which serves to prevent multiple instances of rpd from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

RPD_TASK_REINIT

System Log Message Reinitializing

Description The routing protocol process (rpd) reinitialized.

Type Event: This message reports an event, not an error

Severity info

RPD_TASK_SIGNALIGNORE

System Log Message sigaction(SIG*signal-name*): *error-message*

Description The routing protocol process (rpd) informed the kernel that it wished to ignore the indicated signal, but the kernel failed to process the request.

Type Error: An error occurred

Severity error

RPD_TRACE_FAILED

System Log Message Unable to write to trace file *filename*

Description The routing protocol process (rpd) could not write to the indicated trace file, and stopped attempting to do so. The next commit of the configuration database will reenable tracing.

Type Event: This message reports an event, not an error

Severity error

Chapter 62

RT System Log Messages

This chapter describes messages with the RT prefix. They are generated on routers running the JUNOS software with enhanced services by the Packet Forwarding Engine as it processes packets for security control in real time.

RT_FLOW_SESSION_CLOSE

System Log Message session closed *reason*:
source-address/*source-port*- > *destination-address*/*destination-port*,*protocol-id*:
policy-name, *inbound-packets*(*inbound-bytes*) *outbound-packets*(*outbound-bytes*)
elapsed-time

Description A security session was closed.

Type Event: This message reports an event, not an error

Severity info

RT_FLOW_SESSION_CREATE

System Log Message session created
source-address/*source-port*- > *destination-address*/*destination-port*,*protocol-id*:
policy-name

Description A security session was created.

Type Event: This message reports an event, not an error

Severity info

RT_FLOW_SESSION_DENY

System Log Message session denied
source-address/*source-port*- > *destination-address*/*destination-port*,*protocol-id*(*icmp-type*):
policy-name

Description A security session was not permitted by policy.

Type Event: This message reports an event, not an error

Severity info

RT_H323_CALL_LIMIT_EXCEED

System Log Message Failed to process the packet, active call limit exceeded *maximum-value*

Description The maximum H.323 call limit has been exceeded.

Type Error: An error occurred

Severity error

RT_H323_NAT_COOKIE_NOT_FOUND

System Log Message *object-name* cannot find cookie from session

Description Failed to find the H.323 NAT cookie.

Type Error: An error occurred

Severity error

RT_H323_RAS_REQ_FLOOD

System Log Message RAS Request flood to gatekeeper *destination-address* detected, request threshold *threshold*

Description H.323 Registration Authentication Status request messages have exceeded the configured threshold.

Type Error: An error occurred

Severity error

RT_IPSEC_BAD_SPI

System Log Message IPSec tunnel on int *interface-name* with tunnel ID 0x*tunnel-id* received a packet with a bad SPI. *source-address*-> *destination-address*/*length*, *type*, SPI 0x*index*, SEQ 0x*sequence-number*.

Description Received IPSec packet with bad SPI

Type Error: An error occurred

Severity error

RT_IPSEC_REPLAY

System Log Message Replay packet detected on IPSec tunnel on *interface-name* with tunnel ID 0x*tunnel-id*! From *source-address* to *destination-address*/*length*, *type*, SPI 0x*index*, SEQ 0x*sequence-number*.

Description Received IPSec replay packet

Type Error: An error occurred

Severity error

RT_MGCP_CALL_LIMIT_EXCEED

System Log Message Exceed maximum call *max active call numbermaximum-value*

Description The maximum MGCP active call limit has been exceeded.

Type Error: An error occurred

Severity error

RT_MGCP_DECODE_FAIL

System Log Message Failed to decode MGCP packet

Description Failed to decode MGCP message.

Type Error: An error occurred

Severity error

RT_MGCP_MEM_ALLOC_FAILED

System Log Message Failed to allocate memory for *object-name*

Description Failed to allocate memory for the MGCP objects.

Type Error: An error occurred

Severity error

RT_MGCP_REG_NAT_VEC_FAIL

System Log Message Failed to add MGCP *object-name* to flow module

Description Failed to register the MGCP ALG vector with the flow module.

Type Error: An error occurred

Severity error

RT_MGCP_REG_RM_FAIL

System Log Message Failed to register MGCP ALG with Resource Manager

Description Failed to register the MGCP Resource Manager client.

Type Error: An error occurred

Severity error

RT_MGCP_REM_NAT_VEC_FAIL

System Log Message Failed to remove MGCP *object-name* from flow module

Description Failed to remove the MGCP ALG vector from the flow module.

Type Error: An error occurred

Severity error

RT_MGCP_RM_CLIENTID_FAIL

System Log Message MGCP ALG Resource Manager client registration failed

Description Failed to obtain the MGCP Resource Manager client identifier.

Type Error: An error occurred

Severity error

RT_MGCP_UNREG_BY_RM

System Log Message MGCP ALG client has been unregistered by Resource Manager

Description The Resource Manager has unregistered the MGCP Resource Manager client.

Type Error: An error occurred

Severity error

RT_SCCP_CALL_LIMIT_EXCEED

System Log Message Failed to create SCCP ALG call, call limit *maximum-value* exceeded

Description The maximum SCCP call limit has been exceeded.

Type Error: An error occurred

Severity error

RT_SCCP_CALL_RATE_EXCEED

System Log Message The SCCP active call rate limit *maximum-value* has been exceeded

Description The SCCP active call rate limit has been exceeded.

Type Error: An error occurred

Severity error

RT_SCCP_DECODE_FAIL

System Log Message Failed to decode SCCP packet from *source-address-* > *destination-address*

Description Failed to decode SCCP packet.

Type Error: An error occurred

Severity error

RT_SCCP_NAT_COOKIE_NOT_FOUND

System Log Message Failed to find SCCP ALG cookie from session

Description Failed to find SCCP NAT cookie.

Type Error: An error occurred

Severity error

RT_SCCP_REM_NAT_VEC_FAIL

System Log Message Failed to remove SCCP ALG vector from flow module

Description Failed to remove the SCCP ALG vector from the flow module.

Type Error: An error occurred

Severity error

RT_SCCP_UNREG_RM_FAIL

System Log Message Failed to unregister SCCP client from Resource Manager when the ALG was unregistered

Description Failed to unregister SCCP client from Resource Manager when the ALG was unregistered.

Type Error: An error occurred

Severity error

RT_SCREEN_ICMP

System Log Message *attack-name* source: *source-address*, destination: *destination-address*, zone name: *source-zone-name*, interface name: *interface-name*

Description ICMP attack category

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_ICMP_FLOOD

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description ICMP flood attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_ICMP_FRAG

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description fragmented ICMP packet attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_ICMP_ID

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description ICMP zero ID attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_ICMP_LARGE

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description large ICMP packet attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_ICMP_PING_DEATH

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description ping of death attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP

System Log Message *attack-name* source: *source-address*, destination: *destination-address*, protocol-id: *protocol-id*, zone name: *source-zone-name*, interface name: *interface-name*

Description IP attack category

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_BAD_OPT

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP bad option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_FRAG

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP fragment attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_LAND

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP land attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_OPT_FILTER_ROUTE

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP source route option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_OPT_LSR

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP loose source route option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_OPT_RECORD

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP record route option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_OPT_SCHT

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP security option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_OPT_SSR

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP strict source route option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_OPT_STREAM

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP stream option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_OPT_TIMESTAMP

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP timestamp option attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_SPOOFING

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP spoofing attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_SWEEP

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description IP sweeping attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_IP_UNKNOWN_PROT

System Log Message source: *source-address*, destination: *destination-address*, protocol-id: *protocol-id*zone name: *filter-name*, interface name: *interface-name*

Description IP unknown protocol attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_MAL_URL

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, protocol-id: *protocol-id*zone name: *filter-name*, interface name: *interface-name*

Description malicious URL attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_OVER_SESSION_DST

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description session from the same destination address exceeds the threshold

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_OVER_SESSION_SRC

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description session from the same source address exceeds the threshold

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_PORT_SCAN

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description port scan attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_SESSION_LIMIT

System Log Message *attack-name message*: *ip-address*, zone name: *source-zone-name*, interface name: *interface-name*

Description Session limit category

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_SYN_ACK_ACK

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, zone name: *filter-name*, interface name: *interface-name*

Description SYN-ACK-ACK attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP

System Log Message *attack-name* source: *source-address*:*source-port*, destination: *destination-address*:*destination-port*, zone name: *source-zone-name*, interface name: *interface-name*

Description TCP attack category

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP_DST_IP

System Log Message *attack-name* destination: *destination-address*, zone name: *source-zone-name*, interface name: *interface-name*

Description TCP destination IP attack category

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP_FIN_NO_ACK

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, zone name: *filter-name*, interface name: *interface-name*

Description TCP FIN without ACK flag attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP_FRAG

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, zone name: *filter-name*, interface name: *interface-name*

Description TCP fragment attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP_NO_FLAG

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, zone name: *filter-name*, interface name: *interface-name*

Description TCP no flag attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP_SRC_IP

System Log Message *attack-name* source: *source-address*, zone name: *source-zone-name*, interface name: *interface-name*

Description TCP source IP attack category

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP_SYN_FIN

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, zone name: *filter-name*, interface name: *interface-name*

Description TCP SYN-FIN flag attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TCP_SYN_FLOOD

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, zone name: *filter-name*, interface name: *interface-name*

Description TCP SYN flood attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_TEAR_DROP

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description tear drop attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_UDP

System Log Message *attack-name* source: *source-address*:*source-port*, destination: *destination-address*:*destination-port*, zone name: *source-zone-name*, interface name: *interface-name*

Description UDP attack category

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_UDP_FLOOD

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description UDP flood attack

Type Event: This message reports an event, not an error

Severity error

RT_SCREEN_WINNUKE

System Log Message source: *source-address*, destination: *destination-address*, zone name: *filter-name*, interface name: *interface-name*

Description winnuke attack

Type Event: This message reports an event, not an error

Severity error

RT_SIP_CALL_LIMIT_EXCEED

System Log Message Exceed maximum call

Description The maximum SIP call limit has been exceeded.

Type Error: An error occurred

Severity error

RT_SIP_DECODE_FAIL

System Log Message Failed to decode SIP packet *error-message*

Description Failed to decode incoming SIP packet.

Type Error: An error occurred

Severity error

RT_SIP_INIT_EP_FAIL

System Log Message The SIP stack failed to create an endpoint with the configuration

Description Failed to initialize SIP endpoint.

Type Error: An error occurred

Severity error

RT_SIP_INIT_LISTENER_FAIL

System Log Message The SIP stack failed endpoint failed to create a dummy listener

Description Failed to initialize SIP transport listener.

Type Error: An error occurred

Severity error

RT_SIP_MEM_ALLOC_FAILED

System Log Message Failed to allocate memory for *object-name*

Description Failed to allocate memory from the memory pool.

Type Error: An error occurred

Severity error

RT_SIP_REG_NAT_VEC_FAIL

System Log Message Failed to add SIP ALG vector to flow module

Description Failed to register SIP ALG vector with the flow module.

Type Error: An error occurred

Severity error

RT_SIP_REG_RM_FAIL

System Log Message Failed to register SIP ALG with the Resource Manager

Description Failed to register the SIP ALG Resource Manager client.

Type Error: An error occurred

Severity error

RT_SIP_REM_NAT_VEC_FAIL

System Log Message Failed to remove SIP ALG vector from flow module

Description Failed to remove the SIP ALG vector from the flow module.

Type Error: An error occurred

Severity error

RT_SIP_UNREG_BY_RM

System Log Message SIP client has been unregistered by RM

Description The Resource Manager has notified SIP that a client has been unregistered.

Type Error: An error occurred

Severity error

RT_SOURCE_NAT_ALARM_CLEAR

System Log Message Utilization of source nat pool '*nat-pool-name*' hits clear threshold '*threshold*% %'

Description Utilization of source NAT pool reaches the alarm clear threshold.

Type Error: An error occurred

Severity error

RT_SOURCE_NAT_ALARM_RAISE

System Log Message Utilization of source nat pool '*nat-pool-name*' hits raise threshold '*threshold*% %'

Description Utilization of source NAT pool reaches the alarm raise threshold.

Type Error: An error occurred

Severity error

RT_SRC_NAT_ALARM_CLEAR

System Log Message Utilization of source nat pool '*nat-pool-name*' hits clear threshold '*threshold*% %'

Description Utilization of source NAT pool reaches the alarm clear threshold.

Type Error: An error occurred

Severity error

RT_SRC_NAT_ALARM_RAISE

System Log Message Utilization of source nat pool '*nat-pool-name*' hits raise threshold '*threshold*% %'

Description Utilization of source NAT pool reaches the alarm raise threshold.

Type Error: An error occurred

Severity error

Chapter 63

RTLOG System Log Messages

This chapter describes messages with the RTLOG prefix. They are generated on routers running the JUNOS software with enhanced services by the system log module of the Packet Forwarding Engine as it processes packets for security control in real time.

RTLOG_SOURCE_INIT

System Log Message Log source *service-name* attached at log ring buffer *index*

Description Specified JSR log source is ready to export logs

Type Event: This message reports an event, not an error

Severity info

RTLOG_UTP_TCP_SYN_FLOOD

System Log Message source: *source-address-source-port*, destination: *destination-address-destination-port*, zone name: *filter-name*, interface name: *interface-name*

Description Security LOG UTP fake TCP SYN flood attack.

Type Event: This message reports an event, not an error

Severity error

Chapter 64

RTLOGD System Log Messages

This chapter describes messages with the RTLOGD prefix. They are generated by the system log utility for real-time processing of packets for security control (rtlogd) on routers running the JUNOS software with enhanced services.

RTLOGD_LOG_BIND_ERROR

System Log Message Failed to bind socket to PFE: *error-message*

Description JUNOS JSR log daemon receives JSR log from a JSR log forwarder. The JSR log daemon failed to connect to the forwarder.

Type Error: An error occurred

Severity error

RTLOGD_LOG_READ_ERROR

System Log Message Failed to read from PFE: *error-message*

Description JUNOS JSR log daemon relays JSR logs from the dataplane to the system event daemon for logging. The JSR log daemon fails to read JSR logs for the indicated reason.

Type Error: An error occurred

Severity error

Chapter 65

RTPERF System Log Messages

This chapter describes messages with the RTPERF prefix. They are related to performance logs for the data plane.

RTPERF_CPU_THRESHOLD_EXCEEDED

System Log Message PIC *pic-slot* CPU utilization exceeds threshold, current value = *current-value*

Description PFE cpu threshold exceeded

Type Event: This message reports an event, not an error

Severity critical

RTPERF_CPU_USAGE_OK

System Log Message PIC *pic-slot* CPU utilization returns to normal, current value = *current-value*

Description PFE cpu usage okay

Type Event: This message reports an event, not an error

Severity info

Chapter 66

SAVAL System Log Messages

This chapter describes messages with the SAVAL prefix. They are generated by the MAC SA Validate system (jsavald) process.

SAVAL_RTSOCK_FAILURE

System Log Message Error with rtsock: *error-message*

Description The MAC SA Validate system process (jsavald) experienced the indicated error with a routing socket.

Type Error: An error occurred

Severity info

Cause An internal software failure occurred.

Action Contact your technical support representative.

Chapter 67

SDXD System Log Messages

This chapter describes messages with the SDX prefix. They are generated by the Session and Resource Control (SRC) process (sdxd), which provides a user interface for deploying Internet services.

SDXD_BEEP_FIN_FAIL

System Log Message Graceful close of BEEP session failed

Description The Session and Resource Control (SRC) process (sdxd) could not send a request to the SRC server to close a Blocks Extensible Exchange Protocol (BEEP) session. It sends this request when the session becomes unconfigured.

Type Event: This message reports an event, not an error

Severity notice

Cause The usual cause is that the session was already partially or completely closed.

Action None required. The sdxd process recovers automatically in this situation.

SDXD_BEEP_INIT_FAIL

System Log Message BEEP initialization failed

Description The Session and Resource Control (SRC) process (sdxd) could not initialize the Blocks Extensible Exchange Protocol (BEEP), which it uses to connect to an SRC server.

Type Error: An error occurred

Severity error

Cause An internal software failure might have occurred.

SDXD_CHANNEL_START_FAIL

System Log Message Notification channel could not be started (*error-code*): *message*

Description The indicated Blocks Extensible Exchange Protocol (BEEP) channel could not be started for the indicated reason.

Type Event: This message reports an event, not an error

Severity error

Cause The usual cause is an abnormal operation, which might be described in the system log message.

SDXD_CONNECT_FAIL

System Log Message Connection to SDX server failed: *message*

Description The Session and Resource Control (SRC) process (sdxd) could not connect to an SRC server for the indicated reason.

Type Event: This message reports an event, not an error

Severity notice

Cause There was a network problem or the server was not running.

SDXD_DAEMONIZE_FAIL

System Log Message Aborting, unable to run in the background as a daemon: *error-message*

Description The Service Deployment System process (sdxd) could not create a version of itself to run in the background as a daemon.

Type Error: An error occurred

Severity emergency

SDXD_EVLIB_FAILURE

System Log Message *function-name*: *error-message*

Description The Service Deployment System process (sdxd) called the indicated function in the event library. The function failed with the indicated error.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

SDXD_KEEPALIVES_MISSED

System Log Message No server keepalives received for three intervals

Description The Session and Resource Control (SRC) process (sdxd) and SRC server exchange keepalive messages at regular intervals. The process did not receive a keepalive from the server for three consecutive keepalive intervals. In this case, it closes the session and tries to connect to another SRC server.

Type Event: This message reports an event, not an error

Severity notice

SDXD_KEEPALIVE_SEND_FAIL

System Log Message Unable to send keepalive

Description The Session and Resource Control (SRC) process (sdxd) could not send a keepalive message to the SRC server, which it does periodically to maintain its connection to the server.

Type Event: This message reports an event, not an error

Severity notice

Cause There might have been a network problem.

SDXD_MGMT_SOCKET_IO

System Log Message management daemon I/O failure: *reason*

Description The Service Deployment System process (sdxd) could not read from or write to the management socket that it uses to communicate with the JUNOS management process (mgd).

Type Error: An error occurred

Severity error

Cause The mgd process might have exited abnormally.

SDXD_OUT_OF_MEMORY

System Log Message Insufficient memory during *operation*

Description The Service Deployment System (sdxd) attempted to allocate memory for an internal object during the indicated operation. The attempt failed.

Type Error: An error occurred

Severity error

SDXD_PID_FILE_UPDATE

System Log Message Unable to update process PID file: *error-message*

Description The Service Deployment System process (sdxd) attempted to update the file that records its process ID (PID), which serves to prevent multiple instances of sdxd from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

SDXD_SOCKET_FAILURE

System Log Message *operation* failed: *error-message*

Description The Service Deployment System process (sdxd) uses Transmission Control Protocol (TCP) sockets for communication with the SRC server. The indicated operation, which might be for socket creation or binding to a local address, failed with the indicated error.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

Chapter 68

SNMP System Log Messages

This chapter describes messages with the SNMP prefix. They are generated by two kinds of processes: .

- Processes that perform Simple Network Management Protocol (SNMP) operations, such as the Management Information Base II (MIB II) process (mib2d) and the SNMP agent process (snmpd). Those processes also generate messages with prefixes that match their names, as described in "MIB2D System Log Messages" on page 373 and "SNMPD System Log Messages" on page 513.
- Processes that are instrumented to generate system log messages when they send SNMP traps. The SNMP remote operations process (rmopd) is one such process. It also generates messages with the RMOPD_ prefix, which are described in "RMOPD System Log Messages" on page 419.

SNMP_GET_ERROR1

System Log Message *function-name operation* failed for *object-name*: index1 *index1* (*error-message*)

Description An SNMP Get or GetNext request failed for the indicated object, which has the indicated index.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMP_GET_ERROR2

System Log Message *function-name operation* failed for *object-name*: index1 *index1* index2 *index2* (*error-message*)

Description An SNMP Get or GetNext request failed for the indicated object, which has the indicated indexes.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMP_GET_ERROR3

System Log Message *function-name operation* failed for *object-name*: index1 *index1* index2 *index2* index3 *index3* (*error-message*)

Description An SNMP Get or GetNext request failed for the indicated object, which has the indicated indexes.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMP_GET_ERROR4

System Log Message *function-name operation* failed for *object-name*: index1 *index1* index2 *index2* index3 *index3* index4 *index4* (*error-message*)

Description An SNMP Get or GetNext request failed for the indicated object, which has the indicated indexes.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMP_RTSLIB_FAILURE

System Log Message *function-name*: *reason*: *error-message*

Description A call to the indicated function in the routing socket library failed with the indicated error.

Type Error: An error occurred

Severity emergency

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMP_TRAP_LINK_DOWN

System Log Message ifIndex *snmp-interface-index*, ifAdminStatus *admin-status*, ifOperStatus *operational-status*, ifName *interface-name*

Description The SNMP agent process (snmpd) generated a linkDown trap because the indicated interface changed state to 'down'.

Type Event: This message reports an event, not an error

Severity warning

SNMP_TRAP_LINK_UP

System Log Message ifIndex *snmp-interface-index*, ifAdminStatus *admin-status*, ifOperStatus *operational-status*, ifName *interface-name*

Description The SNMP agent process (snmpd) generated a linkUp trap because the indicated interface changed state to 'up'.

Type Event: This message reports an event, not an error

Severity info

SNMP_TRAP_TRACERT_PATH_CHANGE

System Log Message traceRouteCtlOwnerIndex = *test-owner*, traceRouteCtlTestName = *test-name*

Description The Simple Network Management Protocol (SNMP) remote operations process (rmopd) generated a traceRoutePathChange trap because two probes with the same time-to-live (TTL) value returned with different IP addresses.

Type Event: This message reports an event, not an error

Severity info

SNMP_TRAP_TRACERT_TEST_COMPLETED

System Log Message traceRouteCtlOwnerIndex = *test-owner*, traceRouteCtlTestName = *test-name*

Description The Simple Network Management Protocol (SNMP) remote operations process (rmopd) generated a tracerouteTestCompleted trap because the test completed and the full path to the target was determined.

Type Event: This message reports an event, not an error

Severity info

SNMP_TRAP_TRACERT_TEST_FAILED

System Log Message traceRouteCtlOwnerIndex = *test-owner*, traceRouteCtlTestName = *test-name*

Description The Simple Network Management Protocol (SNMP) remote operations process (rmopd) generated a tracerouteTestFailed trap because the test completed and the full path to the target was not determined.

Type Event: This message reports an event, not an error

Severity info

Chapter 69

SNMPD System Log Messages

This chapter describes messages with the SNMPD prefix. They are generated by the Simple Network Management Protocol (SNMP) agent process (snmpd), which responds to SNMP requests. As necessary, it passes the requests to subagent processes running on its machine and forwards the traps they generate to the SNMP manager.

SNMPD_AUTH_FAILURE

System Log Message *function-name*: *message* from *source-address* to *destination-address* (*index1*)

Description The indicated function failed because the authorization check failed for the interface, Simple Network Management Protocol (SNMP) community, or user making the request.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_AUTH_PRIVILEGES_EXCEEDED

System Log Message *function-name*: *source-address*: request exceeded community privileges

Description The indicated function failed because the Simple Network Management Protocol (SNMP) community making the access request did not have the required privileges.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_AUTH_RESTRICTED_ADDRESS

System Log Message *function-name*: request from address *source-address* not allowed

Description The indicated function failed because access requests from the indicated source address are not allowed.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_AUTH_WRONG_PDU_TYPE

System Log Message *function-name*: *source-address*: unauthorized SNMP PDU type: *pdu-type*

Description The indicated function failed because the indicated type of protocol data unit (PDU) is not supported.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_BIND_INFO

System Log Message Source address for trap socket was set to *bind-address*

Description The source address for the indicated type of socket used by the Simple Network Management Protocol (SNMP) agent process (snmpd) was set to the indicated address.

Type Event: This message reports an event, not an error

Severity info

Cause An administrator changed the JUNOS configuration for the process or for an interface.

Cause The online/offline state changed for a Physical Interface Card (PIC). This can also cause the address to become newly available or unavailable.

SNMPD_CONFIG_ERROR

System Log Message Configuration database has errors

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) detected an error in the SNMP configuration database.

Type Error: An error occurred

Severity error

SNMPD_CONTEXT_ERROR

System Log Message *function-name*: error in *operation* context *context-name*

Description The indicated operation (addition or deletion) failed during configuration of the indicated Simple Network Management Protocol (SNMP) context.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_FILE_FAILURE

System Log Message *function-name*: fopen *filename*: *error-message*

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) could not access the indicated file.

Type Error: An error occurred

Severity emergency

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_GROUP_ERROR

System Log Message *function-name*: error in *operation* group: '*group-id*' user '*username*' model '*model*'

Description The indicated operation (creation, installation, or deletion) failed during configuration of the indicated group.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_HEALTH_MON_THRESH_CROSS

System Log Message *syslog-subtagdelimiterevent-name*

Description A system parameter monitored by the self-monitoring feature crossed a rising or falling threshold.

Type Event: This message reports an event, not an error

Severity error

Cause System resources were being consumed.

SNMPD_INIT_FAILED

System Log Message snmpd initialization failure: *error-message*

Description Initialization of the Simple Network Management Protocol (SNMP) agent process (snmpd) failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_LIBJUNIPER_FAILURE

System Log Message *function-name*: system_default_inaddr: *error-message*

Description The indicated function from the Juniper Networks Simple Network Management Protocol (SNMP) library failed and returned the indicated error to the SNMP agent process (snmpd).

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_RADIX_FAILURE

System Log Message *function-name*: radix_add failed: *error-message*

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) uses radix trees to store valid client prefixes, which are used to determine authorization for requests from users and communities. It could not create a new entry in a radix tree.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_RECEIVE_FAILURE

System Log Message *function-name*: receive message failure: *error-message*

Description The indicated error occurred while the Simple Network Management Protocol (SNMP) agent process (snmpd) was receiving either a protocol data unit (PDU) from the User Datagram Protocol (UDP) or a message from a subagent.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_RMONFILE_FAILURE

System Log Message *function-name*: operation: *operation filename*: *error-message*

Description The indicated operation failed on the indicated remote monitoring (RMON) data file.

Type Error: An error occurred

Severity critical

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_RMON_COOKIE

System Log Message *function-name*: Null cookie

Description An invalid data pointer was returned when the remote monitoring (RMON) asynchronous completion handler performed an RMON alarm operation.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_RMON_EVENTLOG

System Log Message *syslog-subtagdelimitermessage*

Description The indicated remote monitoring (RMON) event completed.

Type Event: This message reports an event, not an error

Severity warning

SNMPD_RMON_MIBERROR

System Log Message *function-name*: internal Get request error: *description*, alarm *alarm-id*, error *error-message*, variable: *name* (*oid*)

Description A Get request for a monitored object instance failed during initialization of the indicated remote monitoring (RMON) alarm.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_RTSLIB_ASYNC_EVENT

System Log Message *function-name*: sequence mismatch (*expected-value*, *received-value*), resyncing

Description A notification from the kernel to the Simple Network Management Protocol (SNMP) agent process (snmpd) was lost.

Type Event: This message reports an event, not an error

Severity notice

SNMPD_SEND_FAILURE

System Log Message *function-name*: send *type* (*index1*) failure: *error-message*

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) could not send either a protocol data unit (PDU) to the User Datagram Protocol (UDP) or a message to a subagent.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_SET_FAILED

System Log Message Snmp set failed: *error-message*

Description Configuration data was changed using an Simple Network Management Protocol (SNMP) Set request, but the SNMP agent process (snmpd) could not save the changes to the configuration database.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_SMOID_GEN_FAILURE

System Log Message Unable to generate OID from *product-name* (*error-message*)

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) could not generate a value for the self-monitoring object identifier (OID) of the indicated product.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_SOCKET_FAILURE

System Log Message *function-name*: socket failure: *reason* (*error-message*)

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) uses sockets for communication with subagents. A socket operation, such as creation or removal, failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_SOCKET_FATAL_FAILURE

System Log Message *function-name*: socket failure: *reason* (*error-message*)

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) uses sockets for communication with subagents. The process exited after a socket operation, such as creation or removal, failed.

Type Error: An error occurred

Severity emergency

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_SYSLIB_FAILURE

System Log Message *function-name*: system function '*system-function-name*' failed: *error-message*

Description The indicated function from the Simple Network Management Protocol (SNMP) system library failed and returned the indicated error to the SNMP agent process (snmpd).

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_SYSOID_FAILURE

System Log Message Unable to determine sysObjectID from internal model: *model*

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) could not determine the value of the sysObjectID object.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_SYSOID_GEN_FAILURE

System Log Message Unable to generate OID for product *product-name* (*error-message*)

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) could not generate a value for the sysObjectID object for the indicated product.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_THROTTLE_QUEUE_DRAINED

System Log Message *function-name*: cleared all throttled traps

Description The queue of throttled traps was cleared.

Type Event: This message reports an event, not an error

Severity info

SNMPD_TRAP_COLD_START

System Log Message *function-name*: SNMP trap: cold start

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) generated a cold-start trap when the entire Routing Engine (including the snmpd process) initialized.

Type Event: This message reports an event, not an error

Severity critical

SNMPD_TRAP_GEN_FAILURE

System Log Message *function-name*: SNMP trap error: *trap-message* (*error-message*)

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) could not generate a trap.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_TRAP_INVALID_DATA

System Log Message *function-name*: SNMP trap error: invalid *message* (*value*) received

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) received a trap message from a subagent that contained an invalid variable binding (varbind) type.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

SNMPD_TRAP_QUEUED

System Log Message Adding trap to *trap-destination* to *queue-name* queue, *size* traps in queue

Description A trap was queued for later transmission.

Type Event: This message reports an event, not an error

Severity info

Cause Possible causes include the following: (a) the system is not completely initialized, (b) a route does not exist, or (c) traps are being throttled.

SNMPD_TRAP_QUEUE_DRAINED

System Log Message *function-name*: traps queued to *trap-destination* sent successfully

Description The queued traps for the indicated destination were successfully sent.

Type Event: This message reports an event, not an error

Severity info

SNMPD_TRAP_QUEUE_MAX_ATTEMPTS

System Log Message *function-name*: after *count* attempts, deleting *trap-count* traps queued to *trap-destination*

Description The number of attempts to send traps to the indicated destination exceeded the configured maximum. The traps still waiting to be sent were discarded.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

SNMPD_TRAP_QUEUE_MAX_SIZE

System Log Message *function-name*: maximum queue size exceeded (*size*), discarding trap to *trap-destination* from *queue-name* queue

Description The number of traps in the trap queue exceeded the configured maximum. The traps still waiting to be sent were discarded.

Type Event: This message reports an event, not an error

Severity info

SNMPD_TRAP_THROTTLED

System Log Message *function-name*: traps throttled after *count* traps

Description The number of traps waiting for transmission exceeded the configured maximum, so the remaining traps were throttled.

Type Event: This message reports an event, not an error

Severity info

SNMPD_TRAP_WARM_START

System Log Message *function-name*: SNMP trap: warm start

Description The Simple Network Management Protocol (SNMP) agent process (snmpd) generated a warm-start trap when it initialized (other Routing Engine processes were already active).

Type Event: This message reports an event, not an error

Severity error

SNMPD_USER_ERROR

System Log Message *function-name*: error in *action* user '*username*' auth '*authentication-type*' priv '*privilege-type*'

Description The indicated operation (creation, installation, or deletion) failed during configuration of the indicated user.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

Chapter 70

SPD System Log Messages

This chapter describes messages with the SPD prefix. They are generated by the adaptive services process (spd), which provides the user interface for management and configuration of Adaptive Services Physical Interface Cards (PICs).

SPD_CONFIGURATION_COMPILE

System Log Message Compilation of configuration rule *rule-name* term *index* failed: *reason*

Description The adaptive services process (spd) could not compile a configured object, such as a rule or rule term.

Type Error: An error occurred

Severity error

SPD_CONN_FATAL_FAILURE

System Log Message Connection attempt failed with fatal error: *error-message*

Description The adaptive services process (spd) attempted to open a connection to an Adaptive Services Physical Interface Card (PIC), to gather information requested in a Simple Network Management Protocol (SNMP) query. The attempt failed with the indicated fatal error.

Type Error: An error occurred

Severity error

SPD_CONN_NO_REPLY

System Log Message *function-name*: no reply from *interface-name* (*error-message*)

Description The adaptive services process (spd) did not receive a reply from the indicated interface on an Adaptive Services Physical Interface Card (PIC) for information requested in a Simple Network Management Protocol (SNMP) query.

Type Error: An error occurred

Severity error

SPD_CONN_OPEN_FAILURE

System Log Message *function-name*: unable to open connection to *interface-name* (*error-message*)

Description The adaptive services process (spd) attempted to open a connection to the indicated interface on an Adaptive Services Physical Interface Card (PIC), to gather information requested in a Simple Network Management Protocol (SNMP) query. The attempt failed for the indicated reason.

Type Error: An error occurred

Severity error

SPD_CONN_SEND_FAILURE

System Log Message *function-name*: unable to send query to *interface-name* (*error-message*)

Description The adaptive services process (spd) attempted to send a request for information, needed for a Simple Network Management Protocol (SNMP) query, to the indicated interface on an Adaptive Services Physical Interface Card (PIC). The attempt failed for the indicated reason.

Type Error: An error occurred

Severity error

SPD_CONN_UNEXPECTED_MSG

System Log Message *function-name*: unexpected response received from *interface-name* (*error-message*)

Description The adaptive services process (spd) sent a request for information, needed for a Simple Network Management Protocol (SNMP) query, to the indicated interface on an Adaptive Services Physical Interface Card (PIC). It received an unexpected response.

Type Error: An error occurred

Severity error

SPD_DAEMONIZE_FAILED

System Log Message Aborting, unable to run in the background as a daemon: *error-message*

Description The adaptive services process (spd) could not create a version of itself to run in the background as a daemon.

Type Error: An error occurred

Severity emergency

SPD_DB_IF_ADD_FAILURE

System Log Message Unable to add database entry for *interface-name*: *error-message*

Description The adaptive services process (spd) uses an internal database to store information needed to reply to Simple Network Management Protocol (SNMP) queries. It could not add an entry to the database for the indicated interface on an Adaptive Services Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

SPD_DB_IF_ALLOC_FAILURE

System Log Message Unable to allocate database entry for *interface-name*: *error-message*

Description The adaptive services process (spd) uses an internal database to store information needed to reply to Simple Network Management Protocol (SNMP) queries. It could not allocate an entry in the database for the indicated interface on an Adaptive Services Physical Interface Card (PIC).

Type Error: An error occurred

Severity error

SPD_DB_SVC_SET_ADD_FAILURE

System Log Message Unable to add database entry for *service-set*: *error-message*

Description The adaptive services process (spd) uses an internal database to store information needed to reply to Simple Network Management Protocol (SNMP) queries. It could not add an entry to the database for the indicated service set.

Type Error: An error occurred

Severity error

SPD_DB_SVC_SET_ALLOC_FAILURE

System Log Message Unable to allocate database entry for *service-set*: *error-message*

Description The adaptive services process (spd) uses an internal database to store information needed to reply to Simple Network Management Protocol (SNMP) queries. It could not allocate an entry in the database for the indicated service set.

Type Error: An error occurred

Severity error

SPD_DUPLICATE

System Log Message Another copy of this program is running

Description An attempt to start the adaptive services process (spd) failed because an instance of the process was already running.

Type Error: An error occurred

Severity error

SPD_EVLIB_CREATE_FAILURE

System Log Message evCreate failed with: *error-message*

Description The adaptive services process (spd) could not create a context used for handling all asynchronous events (such as timers and message availability).

Type Error: An error occurred

Severity emergency

SPD_EVLIB_EXIT_FAILURE

System Log Message evMainLoop return value: *return-value*, error: *error-message*

Description The adaptive services process (spd) returned from an event loop, which it should never do.

Type Error: An error occurred

Severity error

SPD_NOT_ROOT

System Log Message Must be run as root

Description The user who attempted to start the adaptive services process (spd) was not the root user.

Type Error: An error occurred

Severity error

SPD_OUT_OF_MEMORY

System Log Message Insufficient memory for operation *operation*

Description The adaptive services process (spd) attempted to allocate memory for an internal object. The attempt failed.

Type Error: An error occurred

Severity error

SPD_PID_FILE_LOCK

System Log Message Unable to lock PID file: *error-message*

Description The adaptive services process (spd) attempted to lock the file that records its process ID (PID), which serves to prevent multiple instances of spd from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

SPD_PID_FILE_UPDATE

System Log Message Unable to update process PID file: *error-message*

Description The adaptive services process (spd) attempted to update the file that records its process ID (PID), which serves to prevent multiple instances of spd from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

SPD_SERVICE_NEXT_HOP_ADD_FAILED

System Log Message Unable to add service next hop: *error-message* (*error-code*)

Description The adaptive services process (spd) could not add a service next hop for the indicated reason.

Type Error: An error occurred

Severity error

SPD_SERVICE_NEXT_HOP_DEL_FAILED

System Log Message Unable to delete service next hop: *error-message* (*error-code*)

Description The adaptive services process (spd) could not delete a service next hop for the indicated reason.

Type Error: An error occurred

Severity error

SPD_TRAP_OID_GEN_FAILED

System Log Message Unable to generate OID for *identifier* (*error-message*)

Description The adaptive services process (spd) could not generate the indicated object identifier (OID) for a Simple Network Management Protocol (SNMP) trap notification.

Type Error: An error occurred

Severity error

SPD_TRAP_REQUEST_FAILURE

System Log Message *function-name*: *type* request failed: *error-message*

Description The adaptive services process (spd) made the indicated type of request to the application programming interface (API) for generating Simple Network Management Protocol (SNMP) traps, but did not receive the expected result.

Type Error: An error occurred

Severity error

SPD_USAGE

System Log Message Usage: spd [-N] [-v] [-d debug-level]

Description The adaptive services process (spd) displayed the syntax statement for the 'spd' command because the command was invoked incorrectly.

Type Event: This message reports an event, not an error

Severity error

Chapter 71

TASK System Log Messages

This chapter describes messages with the TASK prefix.

TASK_ABORT

System Log Message abort *executable-name*[*pid*] version *version* built by *builder* on *date*: *error-message*

Description The control protocol process terminated because of an internal error.

Type Error: An error occurred

Severity error

Action Examine the messages that immediately follow this message in the system log for information about possible causes.

Cause An internal software failure occurred.

TASK_ACTIVE_TERMINATE

System Log Message Exiting with active tasks: *task-name*

Description After receiving multiple termination requests, the control protocol process exited without performing the indicated cleanup tasks.

Type Event: This message reports an event, not an error

Severity notice

TASK_ASSERT

System Log Message Assertion failed *executable-name*[*pid*]: file "*source-filename*", line *line-number*: "*message*"

Description The source code for this process includes internal self-consistency checks. The process terminated because a check failed, creating a diagnostic core dump for analysis by technical support personnel and noting the number of the line in the source file where the check failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Examine the messages that immediately follow this message in the system log for information about possible causes. Contact a technical support representative, and be ready to provide the list of messages and the diagnostic core dump, if requested.

TASK_ASSERT_SOFT

System Log Message Soft assertion failed *executable-name*[*pid*]: file "*source-filename*", line *line-number*: "*message*", daemon continued running

Description The source code for the process includes internal self-consistency checks. A check failed but the process continued running. It created a diagnostic core dump for analysis by technical support personnel and noted the number of the line in the source file where the check failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Examine the messages that immediately follow this message in the system log for information about possible causes. Contact a technical support representative, and be ready to provide the list of messages and the diagnostic core dump, if requested.

TASK_EXIT

System Log Message Exit *executable-name*[*pid*] version *version* built by *builder* on *date*, caller *address*

Description The process exited, either in response to a user request or because of a system error.

Type Event: This message reports an event, not an error

Severity notice

Cause A system resource was unavailable, an unexpected error occurred, or a user terminated the process.

Action Examine the messages that immediately follow this message in the system log for information about possible causes.

TASK_LOCK_FLOCKED

System Log Message Unable to obtain a lock on *filename*, is another copy of the process running?

Description The process could not obtain the mutual exclusion lock that prevents more than one instance from running simultaneously. The system terminated the indicated process.

Type Error: An error occurred

Severity error

Cause Another process is running.

Action Use the 'show system process' command to verify that another process is running.

TASK_LOCK_LOCKED

System Log Message Unable to obtain a lock on *filename*, *program-name*[*pid*] is still running

Description The process could not obtain the mutual exclusion lock that prevents more than one instance from running simultaneously. The system terminated this instance.

Type Error: An error occurred

Severity error

Cause Another process is running.

Action Use the 'show system process' command to verify that another process is running.

TASK_MGMT_TIMEOUT

System Log Message peer *peer-name* timed out waiting for input

Description Daemon timed out waiting for management input.

Type Error: An error occurred

Severity warning

Action Examine the messages that immediately follow this message in the system log for information about possible causes.

Cause An internal software failure occurred.

TASK_OS_MEMHIGH

System Log Message Using *size* KB of memory, *percentage-value* percent of available

Description The process is using the indicated amount and percentage of Routing Engine memory, which is considered excessive.

Type Error: An error occurred

Severity error

Cause Either the process is leaking memory or the use of system resources is excessive.

Action Increase the amount of RAM in the Routing Engine.

TASK_SCHED_CALLBACK_LONGRUNTIME

System Log Message *function-name*: excessive runtime *time* during *action* of *module*

Description The indicated submodule of this process ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

TASK_SCHED_CUMULATIVE_RUNTIME

System Log Message *function-name*: excessive runtime (total of *time* in *count* callbacks) after *action* of *module*

Description Several submodules of this process ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

TASK_SCHED_MODULE_LONGRUNTIME

System Log Message *function-name*: excessive runtime *time* during *action* of *module*

Description Several submodules of this process ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

TASK_SCHED_TASK_LONGRUNTIME

System Log Message *function-name* ran for *total-time* (*user-time* user, *system-time* system) doing *action*

Description A task callback within this process ran uninterrupted for the indicated period of time, which is considered excessive.

Type Event: This message reports an event, not an error

Severity warning

Cause The duration was noted because task accounting is enabled. The function might be implemented inefficiently.

TASK_SIGNAL_TERMINATE

System Log Message *signal-name* termination signal received

Description In response to the indicated termination request, the process terminated and shut down.

Type Event: This message reports an event, not an error

Severity notice

TASK_START

System Log Message Start *executable-name*[*pid*] version *version* built *date*

Description Process started.

Type Event: This message reports an event, not an error

Severity info

TASK_SYSTEM

System Log Message *reason*: *error-message*

Description A system call made by this process failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request.

TASK_TASK_BEGIN

System Log Message Commencing virtual chassis control daemon, version *process-version*, built *date* by *builder*

Description The process started.

Type Event: This message reports an event, not an error

Severity notice

TASK_TASK_CHILDKILLED

System Log Message *task-name* terminated by SIG*signal-namecore-dump-status*

Description While a child process was performing the indicated operation, it terminated in response to the indicated signal.

Type Event: This message reports an event, not an error

Severity error

TASK_TASK_CHILDSTOPPED

System Log Message *task-name* stopped by SIG*signal-name*

Description While a child process was performing the indicated operation, it stopped in response to the indicated signal.

Type Event: This message reports an event, not an error

Severity error

TASK_TASK_FORK

System Log Message Unable to fork *task-name*: *error-message*

Description This process failed to create the indicated child process.

Type Error: An error occurred

Severity error

TASK_TASK_GETWD

System Log Message getwd: *error-message*

Description The getwd() system call failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request.

TASK_TASK_NOREINIT

System Log Message Reinitialization not possible

Description This process (VCCPD) failed to reinitialize as requested, because it was running in a state that did not allow reconfiguration.

Type Error: An error occurred

Severity error

TASK_TASK_PIDCLOSED

System Log Message Unable to close and remove *filename*: *error-message*

Description This process tried to close and remove the file that records its process ID (PID), which serves to prevent multiple instances from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

TASK_TASK_PIDFLOCK

System Log Message flock(*filename*, LOCK_EX): *error-message*

Description This process issued the flock() system call on the file that records its process ID (PID), which serves to prevent multiple instances from running simultaneously. The system call failed.

Type Error: An error occurred

Severity error

TASK_TASK_PIDWRITE

System Log Message Unable to write *filename*: *error-message*

Description This process tried to write to the file that records its process ID (PID), which serves to prevent multiple instances from running simultaneously. The attempt failed.

Type Error: An error occurred

Severity error

TASK_TASK_REINIT

System Log Message Reinitializing

Description This process reinitialized.

Type Event: This message reports an event, not an error

Severity info

TASK_TASK_SIGNALIGNORE

System Log Message sigaction(SIG*signal-name*): *error-message*

Description This process informed the kernel that it wished to ignore the indicated signal, but the kernel failed to process the request.

Type Error: An error occurred

Severity error

TASK_TRACE_FAILED

System Log Message Unable to write to trace file *filename*

Description This process could not write to the indicated trace file, and stopped attempting to do so. The next commit of the configuration database will reenable tracing.

Type Event: This message reports an event, not an error

Severity error

Chapter 72

TFTPD System Log Messages

This chapter describes messages with the TFTPD prefix. They are generated by the Trivial FTP (TFTP) process (tnp.tftpd), which services requests from hardware components for the configuration files they use during initialization.

TFTPD_AF_ERR

System Log Message Unexpected address family *address-family-type*

Description As each hardware component on the routing platform initializes, it requests its configuration file from the TFTP process (tnp.tftpd). The tnp.tftpd process exited because an incoming packet had the indicated, unexpected value in its address family (sockaddr) field.

Type Error: An error occurred

Severity error

TFTPD_BIND_ERR

System Log Message bind: *error-message*

Description Binding of a socket to an address failed due to a system error.

Type Error: An error occurred

Severity error

TFTPD_CONNECT_ERR

System Log Message connect: *error-message*

Description Connection of a socket to an address failed due to a system error.

Type Error: An error occurred

Severity error

TFTPD_CONNECT_INFO

System Log Message TFTP *operation* from address *address* port *port* file *filename*

Description As each hardware component on the routing platform initializes, it requests its configuration file from the TFTP process (tnp.tftpd). The process established a

connection with the indicated characteristics: kind of operation (read or write), address and port connected to, and name of file transferred.

Type Event: This message reports an event, not an error

Severity info

TFTPD_CREATE_ERR

System Log Message check_space *error-message*

Description The TFTP process (tnp.tftpd) could not create a core dump file.

Type Error: An error occurred

Severity error

Cause There is probably not enough free space in the file system where tnp.tftpd tried to create the file.

TFTPD_FIO_ERR

System Log Message ioctl(FIONBIO): *error-message*

Description The TFTP process (tnp.tftpd) could not set the standard input to be nonblocking.

Type Error: An error occurred

Severity error

TFTPD_FORK_ERR

System Log Message fork: *error-message*

Description As each hardware component on the routing platform initializes, it requests its configuration file from the TFTP process (tnp.tftpd). To service multiple clients simultaneously, tnp.tftpd calls the fork() system call to make a copy of itself for each request. The system call returned the indicated error.

Type Error: An error occurred

Severity error

TFTPD_NAK_ERR

System Log Message nak error *error-code*, *error-message*

Description The TFTP process (tnp.tftpd) sent a negative acknowledgment to a client because of the indicated error condition.

Type Error: An error occurred

Severity warning

TFTPD_OPEN_ERR

System Log Message Unable to open file '*filename*', error: *error-message*

Description The TFTP process (tnp.tftpd) could not open the indicated file because of the indicated error.

Type Error: An error occurred

Severity warning

TFTPD_RECVCOMPLETE_INFO

System Log Message Received *count* blocks of *block-size* size for file '*filename*'

Description The TFTP process (tnp.tftpd) received the last portion of a transmitted file. This message records the number of blocks received, the block size used, and the name of the file to which the data was written.

Type Event: This message reports an event, not an error

Severity info

TFTPD_RECVFROM_ERR

System Log Message recvfrom: *error-message*

Description The TFTP process (tnp.tftpd) issued the recvfrom() system call when attempting to receive data from the network. The system call failed.

Type Error: An error occurred

Severity error

TFTPD_RECV_ERR

System Log Message recv: *error-message*

Description The TFTP process (tnp.tftpd) could not receive data from the network.

Type Error: An error occurred

Severity error

TFTPD_SENDCOMPLETE_INFO

System Log Message Sent *count* blocks of *block-size* and 1 block of *size* for file '*filename*'

Description The TFTP process (tnp.tftpd) successfully sent a file. This message records the number of blocks sent, the block size used, the size of the last block, and the name of the source file.

Type Event: This message reports an event, not an error

Severity info

TFTPD_SEND_ERR

System Log Message send: *error-message*

Description The TFTP process (tnp.tftpd) could not send data.

Type Error: An error occurred

Severity error

TFTPD_SOCKET_ERR

System Log Message socket: *error-message*

Description The TFTP process (tnp.tftpd) could not open a socket for data transmission or reception.

Type Error: An error occurred

Severity error

TFTPD_STATFS_ERR

System Log Message statfs *filename*, error: *error-message*

Description The TFTP process (tnp.tftpd) issued the statfs() system call to obtain the status of the file system into which it needed to write a crash file. The system call failed with the indicated error.

Type Error: An error occurred

Severity error

Chapter 73

UI System Log Messages

This chapter describes messages with the UI prefix. They are generated by the JUNOS command-line interface (CLI) and management process (mgd), which together form the JUNOS user interface that accepts and processes input from users and client applications.

UI_AUTH_EVENT

System Log Message Authenticated user '*username*' at permission level '*authentication-level*'

Description The management process (mgd) authenticated the indicated user.

Type Event: This message reports an event, not an error

Severity info

UI_AUTH_INVALID_CHALLENGE

System Log Message Received invalid authentication challenge for user '*username*': *response*

Description When a user logs onto the routing platform and attempts to authenticate, the CLI and management process (mgd) use a challenge-and-response system to limit the exposure of sensitive information such as passwords and keys. The format of the challenge generated by mgd was incorrect.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_BOOTTIME_FAILED

System Log Message Unable to fetch boot time: *error-message*

Description The management process (mgd) could not retrieve the system boot time from the kernel.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CFG_AUDIT_NEW

System Log Message User '*username*' *action*: *pathname new-name*

Description The indicated user created a new configuration object by copying or renaming an existing object as indicated.

Type Event: This message reports an event, not an error

Severity info

UI_CFG_AUDIT_OTHER

System Log Message User '*username*' *action*: *pathname delimitervalue*

Description The indicated user deleted, activated, or deactivated a configuration object, as indicated. The JUNOS configuration log facility logged the change.

Type Event: This message reports an event, not an error

Severity info

UI_CFG_AUDIT_SET

System Log Message User '*username*' *action*: *pathname delimiterdata* -> "*value*"

Description The indicated user set a value for a configuration object, as indicated.

Type Event: This message reports an event, not an error

Severity info

UI_CFG_AUDIT_SET_SECRET

System Log Message User '*username*' *action*: *pathname*

Description The indicated user set a value for a configuration object, as indicated. For security, the actual value (which might be an authentication key or password, for example) is not recorded.

Type Event: This message reports an event, not an error

Severity info

UI_CHILD_ARGS_EXCEEDED

System Log Message Too many arguments for child process '*command*'

Description The management process (mgd) invokes some commands on behalf of users. It supplied more arguments than the command's syntax statement specifies.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CHILD_CHANGE_USER

System Log Message Unable to switch to local user: *username*

Description The management process (mgd) invokes some commands on behalf of users. Its attempt to adopt the UID of the indicated user failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CHILD_EXEC

System Log Message Child exec failed for command '*command*': *error-message*

Description The management process (mgd) invoked the exec() system call while creating a child processes to execute the indicated command on its behalf. The system call failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CHILD_EXITED

System Log Message Child exited: PID *pid*, status *return-valuecore-dump-status*, command '*command*'

Description The management process (mgd) created a child process to execute the indicated command for it. The child process exited unexpectedly with the indicated status code.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CHILD_FOPEN

System Log Message Unable to append to log '*filename*': *error-message*

Description The management process (mgd) attempted to save the output from a command in the indicated log file, but could not open the file.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CHILD_PIPE_FAILED

System Log Message Unable to create pipe for command '*command*': *error-message*

Description The management process (mgd) created a child process to execute the indicated command for it. Its attempt to create pipes for communication with the child process failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CHILD_STOPPED

System Log Message Child stopped: PID *pid*, signal = *signal-namecore-dump-status*, command = '*command*')

Description The management process (mgd) created a child process to execute the indicated command for it. The child process received the indicated signal and stopped.

Type Error: An error occurred

Severity notice

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CHILD_WAITPID

System Log Message waitpid failed: PID *pid*, rc *return-value*, status *status-code*: *error-message*

Description The management process (mgd) created a child process to execute a command for it. It could not wait for the child process to finish.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_CMDLINE_READ_LINE

System Log Message User '*username*', command '*command*'

Description The indicated user typed the indicated command at the CLI prompt and pressed the Enter key, sending the command string to the management process (mgd).

Type Event: This message reports an event, not an error

Severity info

UI_CMD_AUTH_REGEX_INVALID

System Log Message Invalid '*allow-deny*' command authorization regular expression '*regular-expression*': *error-message*

Description An operation that attempted to set command or configuration authorization included the indicated regular expression. The operation failed because the expression syntax was invalid.

Type Error: An error occurred

Severity error

Action Correct any errors in the regular expression.

UI_COMMIT

System Log Message User '*username*' requested '*command*' operation (comment: *message*)

Description The indicated user requested the indicated type of commit operation on the candidate configuration and added the indicated comment. The 'commit' operation applies to the local Routing Engine and the 'commit synchronize' operation to both Routing Engines.

Type Event: This message reports an event, not an error

Severity notice

UI_COMMIT_AT_ABORT

System Log Message *reason*, will try again

Description An attempt to complete a pending commit operation was cancelled for the indicated reason.

Type Error: An error occurred

Severity error

UI_COMMIT_AT_COMPLETED

System Log Message 'commit at' was successful

Description Changes to the candidate configuration were activated at the time scheduled by a 'commit at' operation.

Type Event: This message reports an event, not an error

Severity notice

UI_COMMIT_AT_FAILED

System Log Message *reason*, scheduled commit cleared

Description A 'commit at' operation did not complete, for the indicated reason.

Type Error: An error occurred

Severity error

UI_COMMIT_COMPRESS_FAILED

System Log Message Unable to compress file '*filename*'

Description As part of committing a new configuration, the management process (mgd) compresses and saves a copy of the configuration. mgd saved the configuration file in regular format because it could not compress it.

Type Error: An error occurred

Severity error

Cause The Routing Engine is low on resources.

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_COMMIT_CONFIRMED_REMINDER

System Log Message 'commit confirmed' must be confirmed within *duration* minutes

Description A 'commit confirmed' operation has activated the candidate configuration temporarily. If the commit is not confirmed within the indicated number of minutes (for example, by the command-line interface (CLI) 'commit' command), the management process (mgd) will roll back to the previous configuration.

Type Event: This message reports an event, not an error

Severity notice

UI_COMMIT_EMPTY_CONTAINER

System Log Message Skipped empty object '*node-name*'

Description Some container objects are marked for automatic removal from the configuration hierarchy if they are empty when the user who created them changes to the top ([edit]) level of the hierarchy or exits configuration mode. While committing the candidate configuration, the management process (mgd) encountered such an object that was empty but not removed.

Type Event: This message reports an event, not an error

Severity info

Cause When the commit operation began, the user who created the new container object had not populated it and was in configuration mode but not at the top level of the hierarchy.

Action Populate or remove the empty object before committing the configuration. The user who created the object can remove it by exiting configuration mode or issuing the 'top' command to move to the top level of the hierarchy.

UI_COMMIT_NOT_CONFIRMED

System Log Message Commit was not confirmed; *message*

Description The 'commit confirmed' operation commits a configuration but requires confirmation within a defined number of minutes for the commit to become permanent. If the commit is not confirmed (by the 'commit' command, for example), the management process (mgd) automatically rolls back to the previously committed configuration. The automatic rollback restores management access to the routing platform in case an error in the configuration blocks access.

Type Event: This message reports an event, not an error

Severity notice

UI_COMMIT_PROGRESS

System Log Message Commit operation in progress: *message*

Description As it performed a commit operation, the management process (mgd) recorded its execution of the indicated step.

Type Event: This message reports an event, not an error

Severity info

UI_COMMIT_ROLLBACK_FAILED

System Log Message Automatic rollback failed

Description The 'commit confirmed' operation commits a configuration but requires confirmation within a defined number of minutes for the commit to become permanent. If the commit is not confirmed (by the 'commit' command, for example), the management process (mgd) automatically rolls back to the previously committed configuration. The 'commit confirmed' operation was not confirmed, but mgd could not roll back the configuration. The configuration might be in an indeterminate state.

Type Error: An error occurred

Severity error

Cause The cause of the problem might be recorded in messages that precede this message in the system log.

UI_COMMIT_SYNC_FORCE

System Log Message All logins to local configuration database were terminated because forced 'commit synchronize' operation was invoked on other Routing Engine

Description The 'commit synchronize force' command was issued on the other Routing Engine on the router. All login sessions in the local configuration database were terminated and the configuration from the other Routing Engine was committed on the local Routing Engine.

Type Event: This message reports an event, not an error

Severity notice

UI_CONFIGURATION_ERROR

System Log Message Process: *process-name*, path: *pathname*, statement: *configuration-statement*, *error-message*

Description The indicated process found a problem in its configuration.

Type Error: An error occurred

Severity error

UI_CONFIGURATION_WARNING

System Log Message Process: *process-name*, path: *pathname*, statement: *configuration-statement*, *warning-message*

Description The indicated process found a problem in its configuration.

Type Error: An error occurred

Severity warning

UI_DAEMON_ACCEPT_FAILED

System Log Message *connection-type* socket connection accept failed: *error-message*

Description The management process (mgd) did not accept an incoming connection request.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_DAEMON_FORK_FAILED

System Log Message Unable to create session child: *error-message*

Description The management process (mgd) invokes the fork() system call to create a copy of itself for each CLI session. The system call failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_DAEMON_SELECT_FAILED

System Log Message select failed: *error-message*

Description The management process (mgd) uses the select() system call to listen for incoming connection requests on a socket. The system call failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_DAEMON_SOCKET_FAILED

System Log Message *connection-type* socket create failed: *error-message*

Description The management process (mgd) uses sockets to communicate with other JUNOS software processes running on the routing platform. It could not allocate a socket.

Type Error: An error occurred

Severity error

Cause System resources are exhausted.

Action Contact your technical support representative.

UI_DBASE_ACCESS_FAILED

System Log Message Unable to reaccess configuration database file '*filename*', address *address*, size *size*: *reason*

Description To increase the size of the configuration database, the management process (mgd) must unmap the database from its address space, change the database size, and remap the database. The remapping operation failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_DBASE_CHECKOUT_FAILED

System Log Message Database '*filename*' is out of data and needs to be rebuilt

Description When the routing platform boots, the management process (mgd) checks the configuration database for internal consistency. It found one or more inconsistencies.

Type Event: This message reports an event, not an error

Severity alert

Cause mgd restarted after new JUNOS software was installed.

Action None; mgd will rebuild the database.

UI_DBASE_EXTEND_FAILED

System Log Message Unable to extend configuration database file '*filename*' to size *requested-size*: *reason*

Description The management process (mgd) could not increase the configuration database to the indicated size.

Type Error: An error occurred

Severity error

Cause The hard disk is defective or is not installed in the routing platform.

Action Repair or replace the hard disk.

Cause There is insufficient disk space on the /var partition on the hard disk.

Action Delete user files from the /var/homes directory to increase the available disk space.

UI_DBASE_LOGIN_EVENT

System Log Message User '*username*' entering configuration mode

Description The indicated user entered configuration mode (logged into the configuration database).

Type Event: This message reports an event, not an error

Severity notice

UI_DBASE_LOGOUT_EVENT

System Log Message User '*username*' exiting configuration mode

Description The indicated user exited configuration mode (logged out of the configuration database).

Type Event: This message reports an event, not an error

Severity notice

UI_DBASE_MISMATCH_EXTENT

System Log Message Database header extent mismatch for file '*filename*': expecting *expected-value*, got *received-value*

Description The header in the configuration database records the highest address allocated in the database. The management process (mgd) discovered that the highest address actually allocated in the database does not match the header value.

Type Error: An error occurred

Severity error

Cause The database file is corrupted.

Action Contact your technical support representative.

UI_DBASE_MISMATCH_MAJOR

System Log Message Database header major version number mismatch for file '*filename*': expecting *expected-value*, got *received-value*

Description For compatibility, the version number recorded in the header of the configuration database must match the version of JUNOS software running on the routing platform. The management process (mgd) discovered that the major parts (for example, '5' in '5.x') of the version numbers do not match.

Type Error: An error occurred

Severity error

Cause A recent software upgrade did not complete successfully.

Action Issue the 'show version' command to check the JUNOS version. If necessary, issue the 'request system reboot' command to reboot the routing platform and complete the software installation.

Cause The database file is corrupted.

Action Contact your technical support representative.

UI_DBASE_MISMATCH_MINOR

System Log Message Database header minor version number mismatch for file '*filename*': expecting *expected-value*, got *received-value*

Description For compatibility, the version number recorded in the header of the configuration database must match the version of JUNOS software running on the routing platform. The management process (mgd) discovered that the minor parts (for example, '2' in 'x.2') of the version numbers do not match.

Type Error: An error occurred

Severity error

Cause A recent software upgrade did not complete successfully.

Action Issue the 'show version' command to check the JUNOS version. If necessary, issue the 'request system reboot' command to reboot the routing platform and complete the software installation.

Cause The database file is corrupted.

Action Contact your technical support representative.

UI_DBASE_MISMATCH_SEQUENCE

System Log Message Database header sequence numbers mismatch for file '*filename*'. If a package has just been added or deleted, please verify and commit the configuration.

Description The header of the configuration database records the version number of the configuration schema (possible set of statements) used when the database was created. To prevent corruption, all JUNOS processes that access the database must use the same schema. The management process (mgd) discovered that the version number for the JUNOS software installed on the routing platform does not match the header value.

Type Error: An error occurred

Severity warning

Cause A recent software upgrade did not complete successfully.

Action Issue the 'show version' command to check the JUNOS version. If necessary, issue the 'request system reboot' command to reboot the routing platform and complete the software installation.

Cause The database file is corrupted.

Action Contact your technical support representative.

UI_DBASE_MISMATCH_SIZE

System Log Message Database header size mismatch for file '*filename*': expecting *expected-value*, got *received-value*

Description The header of the configuration database records the database size. The management process (mgd) discovered that the size of the actual database file does not match the header value.

Type Error: An error occurred

Severity error

Cause The database file is corrupted.

Action Contact your technical support representative.

UI_DBASE_OPEN_FAILED

System Log Message Database open failed for file '*filename*': *reason*

Description The management process (mgd) could not open the indicated configuration database file.

Type Error: An error occurred

Severity error

Cause The database file does not exist.

Action Select a different filename or create a new configuration.

Cause The /config directory does not have sufficient space for a new database.

Action Remove files from the /config directory to make more space available.

UI_DBASE_REBUILD_FAILED

System Log Message *modeusername* rebuild of the database '*filename*' failed

Description The management process (mgd) could not rebuild the configuration database file.

Type Error: An error occurred

Severity alert

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_DBASE_REBUILD_SCHEMA_FAILED

System Log Message Automatic rebuild of the database failed

Description The management process (mgd) could not rebuild the schema for the configuration database.

Type Error: An error occurred

Severity alert

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_DBASE_REBUILD_STARTED

System Log Message *modeusername* rebuild/rollback of the database '*filename*' started

Description The management process (mgd) began to rebuild the configuration database file or its schema because that object was not current. The operation will complete shortly.

Type Event: This message reports an event, not an error

Severity alert

UI_DBASE_RECREATE

System Log Message User '*username*' attempting database re-creation

Description The management process (mgd) discovered that the version of JUNOS software running on the routing platform does not match the version of the current configuration database. In response to a prompt from mgd, the indicated user initiated a rebuilding of the database.

Type Event: This message reports an event, not an error

Severity notice

UI_DBASE_REOPEN_FAILED

System Log Message Reopen of the database failed

Description After rebuilding the schema file for the configuration database, the management process (mgd) closes the file and reopens it in read-only mode to prevent corruption. It could not reopen the file.

Type Error: An error occurred

Severity alert

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_DUPLICATE_UID

System Log Message Users *username1* and *username2* have the same UID *uid*

Description The JUNOS software allows multiple user login accounts to share the same UID. This message was logged in case site policy dictates that users should not share UIDs.

Type Event: This message reports an event, not an error

Severity notice

Action Assign different UIDs to the affected users.

UI_FACTORY_OPERATION

System Log Message Committing factory default configuration because CONFIG button was pressed and held

Description The management process (mgd) began a commit operation to activate the factory default configuration, because the CONFIG button on the chassis was pressed and held for 15 seconds or more.

Type Event: This message reports an event, not an error

Severity notice

UI_INITIALSETUP_OPERATION

System Log Message Committing EZsetup configuration as EZsetup option is chosen

Description The management process (mgd) began a commit operation to activate the pre initial setup configuration, because the initial-setup option was selected from the LCD Menu.

Type Event: This message reports an event, not an error

Severity notice

UI_INVALID_REMOTE_PERMISSION

System Log Message invalid permissions from authorization server: *permission-name*

Description RADIUS and TACACS+ authorization servers use Juniper Networks vendor-specific attributes (VSAs) to specify user permissions. A VSA included the indicated permission name, which is invalid.

Type Error: An error occurred

Severity error

UI_JUNOSCRIPT_CMD

System Log Message User '*username*' used JUNOScript client to run command '*command*'

Description The indicated user ran the indicated command using the JUNOScript application programming interface (API).

Type Event: This message reports an event, not an error

Severity info

UI_JUNOSCRIPT_ERROR

System Log Message JUNOScript error: *error-message*

Description The management process (mgd) normally sends an error message to the JUNOS CLI or JUNOScript API client in an <xnm:error> tag. It could not send the tag, so it sent the indicated error message in an XML comment instead.

Type Error: An error occurred

Severity warning

UI_LCC_NO_MASTER

System Log Message No master Routing Engine defined for LCC*lcc*

Description By default, the JUNOS software installed on the TX Matrix platform in a routing matrix is automatically copied to and installed on all T640 routing nodes in the routing matrix. The software was not installed on the indicated T640 routing node (line-card chassis, or LCC), because the management process (mgd) on the TX Matrix platform could not determine which Routing Engine on the LCC was the master.

Type Error: An error occurred

Severity error

Action Resolve the mastership situation on the T640 routing node and install the software on its Routing Engines.

UI_LOAD_EVENT

System Log Message User '*username*' is performing a '*operation*'

Description The indicated user requested the indicated operation ('rollback, ' or 'load' or one of its variants) on the configuration database. The existing configuration database was deleted and a new database was created based on a text file.

Type Event: This message reports an event, not an error

Severity notice

UI_LOAD_JUNOS_DEFAULT_FILE_EVENT

System Log Message Loading the default config from *pathname*

Description The system is loading junos default configuration from file.

Type Event: This message reports an event, not an error

Severity info

UI_LOGIN_EVENT

System Log Message User '*username*' login, class '*class-name*' *local-peer*[*pid*]

Description The indicated user started a JUNOS CLI session.

Type Event: This message reports an event, not an error

Severity info

UI_LOGOUT_EVENT

System Log Message User '*username*' logout

Description The indicated user exited from a JUNOS CLI session.

Type Event: This message reports an event, not an error

Severity info

UI_LOST_CONN

System Log Message Lost connection to daemon '*process-name*'

Description The management process (mgd) uses sockets to communicate with other JUNOS software processes. The socket it was using for the indicated process closed prematurely.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_MASTERSHIP_EVENT

System Log Message *mastership-event card-name* mastership by '*username*'

Description Some redundant routing platform components use a master/standby system in which the master component is active and the standby is inactive but ready to assume mastership. The indicated user performed the indicated operation to modify component mastership.

Type Event: This message reports an event, not an error

Severity warning

UI_MGD_TERMINATE

System Log Message Terminating operation: exit status *return-value*

Description The management process (mgd) encountered an error and exited, returning the indicated code as its exit status code.

Type Error: An error occurred

Severity error

Cause The cause of the problem might be recorded in messages that precede this message in the system log.

UI_MOTD_PROPAGATE_ERROR

System Log Message Unable to propagate login announcement (motd) to *pathname*

Description The management process (mgd) could not create or write to the indicated file, which was the intended location for the message of the day (MOTD) configured at the [edit system login announcement] hierarchy level.

Type Error: An error occurred

Severity error

UI_NETCONF_CMD

System Log Message User '*username*' used NETCONF client to run command '*command*'

Description The indicated user ran the indicated command using the NETCONF application programming interface (API).

Type Event: This message reports an event, not an error

Severity info

UI_NETCONF_ERROR

System Log Message NETCONF error: *error-message*

Description The management process (mgd) normally sends error messages to the NETCONF client in the <rpc-error> tag element. It could not send that tag element, and instead sent the indicated error message in an XML comment.

Type Error: An error occurred

Severity warning

UI_PARSE_JUNOSCRIPT_ATTRIBUTES

System Log Message Error parsing attributes in client *junoscript* tag

Description The management process (mgd) encountered an error and exited while attempting to parse the XML attributes in the <junoscript> tag submitted by a client application.

Type Error: An error occurred

Severity error

UI_READ_FAILED

System Log Message read failed for peer *peer-name*: *error-message*

Description The management process (mgd) uses the read() system call to access data sent by other JUNOS processes running on the routing platform (referred to as its peers). The system call failed for the indicated process.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_READ_TIMEOUT

System Log Message Timeout on read of peer '*peer-name*'

Description When communicating with other JUNOS processes running on the routing platform (referred to as peers), the management process (mgd) waits only a defined period for responses to arrive. The timeout period passed for the indicated process.

Type Event: This message reports an event, not an error

Severity notice

UI_REBOOT_EVENT

System Log Message System *halt-reboot* by '*username*'

Description The indicated software process restarted as requested by the indicated user.

Type Event: This message reports an event, not an error

Severity warning

UI_RESCUE_OPERATION

System Log Message Committing rescue configuration because CONFIG button was pressed

Description The management process (mgd) began a commit operation to activate the rescue configuration, because the CONFIG button on the chassis was pressed.

Type Event: This message reports an event, not an error

Severity notice

UI_RESTART_EVENT

System Log Message User '*username*' restarting daemon '*process-name*'*description*

Description The indicated software process restarted as requested by the indicated user.

Type Event: This message reports an event, not an error

Severity warning

UI_SCHEMA_CHECKOUT_FAILED

System Log Message Schema is out of date and needs to be rebuilt

Description The JUNOS user interface schema file records all CLI commands and configuration statements available in the JUNOS software. While initializing, the new management process (mgd) determined that the schema's sequence number means that the schema is incompatible with the JUNOS software installed on the routing platform.

Type Error: An error occurred

Severity alert

Cause The schema is out of date.

Action None; mgd will rebuild the schema based on the current JUNOS version.

UI_SCHEMA_MISMATCH_MAJOR

System Log Message Schema major version mismatch for package *package-name* (*expected-value* vs. *received-value*)

Description The JUNOS user interface schema file records all CLI commands and configuration statements available in the JUNOS software. While initializing, the management process (mgd) discovered that the major part (for example, '5' in '5.x') of the schema version number does not match the major version number of the JUNOS software installed on the routing platform. The mismatch could lead to corruption of the configuration database.

Type Error: An error occurred

Severity error

Cause The schema is incompatible with the installed JUNOS software.

Action None; mgd will rebuild the schema based on the current JUNOS version.

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_SCHEMA_MISMATCH_SEQUENCE

System Log Message Schema header sequence numbers mismatch for package *package-name*

Description The JUNOS user interface schema file records all CLI commands and configuration statements available in the JUNOS software. Schema sequence numbers serve as a checksum of the configuration data schema and ensure that the software used to access the database understands the data. The value in the database file did not match the expected value.

Type Error: An error occurred

Severity error

Cause The JUNOS software installation did not succeed, possibly because of an internal software error.

Action Contact your technical support representative.

UI_SCHEMA_SEQUENCE_ERROR

System Log Message Schema sequence number mismatch

Description The JUNOS user interface schema file records all CLI commands and configuration statements available in the JUNOS software. The management process (mgd) rebuilds the schema as necessary to be compatible with the JUNOS software installed on the routing platform. A sequence number in the schema acts as a checksum that represents its content and format. A JUNOS process attempted to access the schema but determined that the schema's sequence number means that it is incompatible with the process.

Type Error: An error occurred

Severity alert

Cause An internal software failure occurred.

Action Contact your technical support representative.

UI_TACPLUS_ERROR

System Log Message TACACS+ failure: *error-message*

Description The management process (mgd) failed to send a record to TACACS+.

Type Error: An error occurred

Severity notice

UI_VERSION_FAILED

System Log Message Unable to fetch system version: *error-message*

Description The management process (mgd) could not retrieve version information from the kernel.

Type Error: An error occurred

Severity error

Action Contact your technical support representative.

UI_WRITE_RECONNECT

System Log Message Re-establishing connection to peer '*peer-name*'

Description The management process (mgd) reconnected to the indicated JUNOS process running on the routing platform.

Type Event: This message reports an event, not an error

Severity notice

Chapter 74

VCCPD System Log Messages

This chapter describes messages with the VCCPD prefix. They are generated by the virtual chassis control protocol (vccpd) process.

VCCPD_KNL_VERSION

System Log Message Routing socket version mismatch (kernel *kernel-version* ! = vccpd *version*) -- kernel upgrade required

Description The virtual chassis control protocol process (VCCPD) discovered that the kernel does not support the version of routing sockets it requires.

Type Error: An error occurred

Severity error

Cause The kernel version is older than the VCCPD version.

Action Upgrade the kernel package.

VCCPD_KNL_VERSIONNONE

System Log Message Routing socket message type *message-type*'s version is not supported by kernel, expected *version* -- kernel upgrade required

Description The virtual chassis control protocol process (VCCPD) discovered that the kernel does not support the routing socket message types that it requires.

Type Error: An error occurred

Severity error

Cause The kernel version is older than the VCCPD version.

Action Upgrade the kernel package.

VCCPD_KNL_VERSIONOLD

System Log Message Routing socket message type *message-type*'s version is older than expected (*kernel-version* < *version*) -- consider upgrading the kernel

Description The virtual chassis control protocol process (VCCPD) discovered that the kernel uses an older version of routing socket message types than it does.

Type Error: An error occurred

Severity error

Cause The kernel version is older than the VCCPD version.

Action Upgrade the kernel package.

VCCPD_PROTOCOL_ADJDOWN

System Log Message Lost adjacency to *neighbor-system-id*s on *interface-name*,

Description A virtual chassis adjacency with the indicated neighboring switch was terminated. The local switch no longer exchanges information with the neighboring switch.

Type Event: This message reports an event, not an error

Severity notice

Cause The communication path to the neighboring switch was disrupted, a protocol error occurred, or the neighboring switch was powered down.

VCCPD_PROTOCOL_ADJUP

System Log Message New adjacency to *neighbor-system-id*s on *interface-name*

Description A virtual chassis adjacency was established with the indicated neighboring switch. The local switch can now exchange information with it.

Type Event: This message reports an event, not an error

Severity info

VCCPD_PROTOCOL_LSPCKSUM

System Log Message LSP checksum error, interface *interface-name*, LSP id *lsp*l, sequence *sequence-number*, checksum *checksum*, lifetime *duration*

Description The indicated vccpd link-state PDU (LSP) failed an internal checksum validity test, implying that it was corrupted.

Type Error: An error occurred

Severity warning

Cause The packet was corrupted in transit between the neighboring switch and this switch, or memory on one of the switches was corrupted.

Action None, unless a large number of these messages appear in the system log file. The corrupted LSP is purged from the virtual chassis and sent again by the originator.

VCCPD_PROTOCOL_OVERLOAD

System Log Message vccpd database overload

Description The vccpd link-state database is full and no additional memory can be allocated for it.

Type Error: An error occurred

Severity alert

Cause No additional memory is available for storing vccpd link-state information. Either system resources are exhausted or a software error occurred (such as a memory leak).

Action Perform one or more of the following actions: (1) Check for unusually high memory usage by vccpd, (2) Add more memory to the switch.

VCCPD_SYSTEM

System Log Message *reason*: *error-message*

Description A system call made by this process failed.

Type Error: An error occurred

Severity error

Cause It is possible that the kernel lacked the resources to fulfill the request.

Chapter 75

VRRPD System Log Messages

This chapter describes messages with the VRRPD prefix. They are generated by the Virtual Router Redundancy Protocol (VVRP) process (vrrpd), which provides the user interface for management of VRRP groups.

VRRPD_ADVERT_TIME_MISMATCH

System Log Message Packet received by *interface-name* for VRRP group *vrrp-group-id* had advertisement time *received-value* ms instead of required *expected-value* ms

Description A Virtual Routing Redundancy Protocol (VRRP) advertisement packet received by the indicated interface for the indicated VRRP group specified an advertisement-timer value different from the value configured for the interface and group. The advertisement interval must be the same on all routing platforms in the VRRP group. For VRRP with IPv4, the value is set by the 'advertise-interval <seconds>' or 'fast-interval <milliseconds>' statement at the [edit interfaces <interface-name> unit <logical-unit-number> family inet address <address> vrrp-group <group-number>] hierarchy level. For VRRP with IPv6, the value is set by the 'inet6-advertise-interval <seconds>' or 'fast-interval <milliseconds>' statement at the [edit interfaces <interface-name> unit <logical-unit-number> family inet6 address <address> vrrp-inet6-group <group-number>] hierarchy level.

Type Error: An error occurred

Severity error

VRRPD_AUTH_INFO_INVALID

System Log Message VRRP ad packet from *ip-address* received by interface *interface-name.interface-unit* for group *vrrp-group-id* was invalid: *error-message*

Description The Virtual Routing Redundancy Protocol (VRRP) advertisement packet sent from the indicated IP address and received by the VRRP process (vrrpd) for the indicated group at the indicated address contained invalid authentication information. The message 'invalid-authentication-type' means that the packet specifies an authentication type that is not defined in RFC 2338, Virtual Router Redundancy Protocol. The message 'authentication-type-mismatch' means that the packet specifies an authentication type different from the type used by the interface that received the packet. The message 'authentication-key-mismatch' means that the authentication key in the packet is incorrect.

Type Error: An error occurred

Severity warning

VRRPD_GET_TRAP_HEADER_FAILED

System Log Message Request for trap signature header failed

Description The Virtual Routing Redundancy Protocol (VRRP) process requested the signature header for an SNMP trap. The request failed.

Type Error: An error occurred

Severity error

Cause An internal software failure occurred.

VRRPD_LINK_LOCAL_ADD_MISMATCH

System Log Message Link-Local Address Mismatch: *received-value expected-value*

Description The indicated interface received a Virtual Routing Redundancy protocol (VRRP) packet for the indicated VRRP group in which the link-local address was different from the one configured for the group and interface

Type Error: An error occurred

Severity error

VRRPD_MISSING_VIP

System Log Message Packet received by *interface-name* for VRRP group *vrrp-group-id* did not include required virtual IP address *ip-address*

Description The indicated interface received a Virtual Routing Redundancy protocol (VRRP) packet for the indicated VRRP group in which the list of virtual IP addresses did not include the indicated address. For VRRP with IPv4, the list is defined by the 'virtual-address [<addresses>]' statement at the [edit interfaces <interface-name> unit <logical-unit-number> family inet address <address> vrrp-group <group-number>] hierarchy level. For VRRP with IPv6, the list is defined by the 'virtual-inet6-address [<addresses>]' statement at the [edit interfaces <interface-name> unit <logical-unit-number> family inet6 address <address> vrrp-inet6-group <group-number>] hierarchy level.

Type Error: An error occurred

Severity error

VRRPD_NEW_BACKUP

System Log Message Interface *interface-name.interface-unit* (local address *interface-address*) became VRRP backup for group *vrrp-group-id*

Description The indicated interface became the Virtual Routing Redundancy Protocol (VRRP) backup for the indicated VRRP group. The VRRP process (vrrpd) stopped sending VRRP advertisements for the virtual IP address on the interface that corresponds to the group.

Type Event: This message reports an event, not an error

Severity warning

VRRPD_NEW_MASTER

System Log Message Interface *interface-name.interface-unit* (local address *interface-address*) became VRRP master for group *vrrp-group-id*

Description The indicated interface became the Virtual Routing Redundancy Protocol (VRRP) master for the indicated VRRP group. The VRRP process (vrrpd) started sending VRRP advertisements for the virtual IP address on the interface that corresponds to the group.

Type Event: This message reports an event, not an error

Severity warning

VRRPD_VIP_COUNT_MISMATCH

System Log Message Packet received by *interface-name* for VRRP group *vrrp-group-id* had *received-value* virtual IP addresses instead of required *expected-value*

Description The indicated interface received a Virtual Routing Redundancy Protocol (VRRP) packet for the indicated VRRP group in which the number of virtual IP addresses was different from the number of addresses configured for the group and interface. The list of addresses must be the same on all routing platforms in a VRRP group. For VRRP with IPv4, the list is defined by the 'virtual-address [<addresses>]' statement at the [edit interfaces <interface-name> unit <logical-unit-number> family inet address <address> vrrp-group <group-number>] hierarchy level. For VRRP with IPv6, the list is defined by the 'virtual-inet6-address [<addresses>]' statement at the [edit interfaces <interface-name> unit <logical-unit-number> family inet6 address <address> vrrp-inet6-group <group-number>] hierarchy level.

Type Error: An error occurred

Severity error

Chapter 76

WEB System Log Messages

This chapter describes messages with the WEB prefix. They are generated by the Hypertext Transfer Protocol process (httpd), which provides a graphical user interface (GUI) for monitoring and configuring J-series Services Routers.

WEB_AUTH_FAIL

System Log Message Unable to authenticate httpd client (username *username*)

Description The checklogin authentication process could not authenticate the indicated user.

Type Event: This message reports an event, not an error

Severity notice

WEB_AUTH_SUCCESS

System Log Message Authenticated httpd client (username *username*)

Description The checklogin authentication process authenticated the indicated user.

Type Event: This message reports an event, not an error

Severity notice

WEB_AUTH_TIME_EXCEEDED

System Log Message Login attempt exceeded maximum processing time

Description The checklogin process halted a login attempt because it took longer than the maximum processing time allowed.

Type Error: An error occurred

Severity error

WEB_CERT_FILE_NOT_FOUND

System Log Message Could not find certificate file '*filename*', disabling HTTPS

Description http-gk could not open the configured HTTPS certificate for reading.

Type Error: An error occurred

Severity error

WEB_CHILD_STATE

System Log Message Unable to retrieve child state: *error-message*

Description The Web management process (httpd) could not retrieve state information for a child process that had exited, for the indicated reason.

Type Error: An error occurred

Severity error

WEB_CONFIG_OPEN_ERROR

System Log Message Could not open '*filename*' for writing

Description httpd-gk could not open the web server configuration file for writing.

Type Error: An error occurred

Severity error

WEB_CONFIG_WRITE_ERROR

System Log Message Could not write '*filename*' configuration. Disk full?

Description httpd-gk could not write the web server configuration file to disk.

Type Error: An error occurred

Severity error

WEB_COULDNT_START_HTTPD

System Log Message Could not fork httpd process!

Description The Web management gatekeeper process (httpd-gk) could not start the web management process (httpd).

Type Error: An error occurred

Severity error

WEB_EVENTLIB_INIT

System Log Message Unable to initialize event library: *error-message*

Description The Web management gatekeeper process (httpd-gk) attempted to initialize the event library during startup. The attempt failed for the indicated reason.

Type Error: An error occurred

Severity error

WEB_KEYPAIR_FILE_NOT_FOUND

System Log Message Could not find key pair file '*filename*', disabling HTTPS

Description http-gk could not open the configured HTTPS key pair file for reading.

Type Error: An error occurred

Severity error

WEB_MGD_BIND_ERROR

System Log Message Could not bind mgd listener socket: *error-message*

Description The web management process could not open the MGD listening socket.

Type Error: An error occurred

Severity error

WEB_MGD_CHMOD_ERROR

System Log Message Could not chmod mgd listener socket

Description The web management process could not change the MGD listening socket to proper file permissions.

Type Error: An error occurred

Severity error

WEB_MGD_CONNECT_ERROR

System Log Message Could not connect to mgd management socket

Description The web management process could not connect to the MGD management socket.

Type Error: An error occurred

Severity error

WEB_MGD_FCNTL_ERROR

System Log Message Could not set incoming mgd request to nonblocking

Description The web management process could not set the MGD listening socket to nonblocking.

Type Error: An error occurred

Severity error

WEB_MGD_LISTEN_ERROR

System Log Message Could not listen mgd listener socket: *error-message*

Description The web management process could not open the MGD listening socket.

Type Error: An error occurred

Severity error

WEB_MGD_RECVMSG_PEEK_ERROR

System Log Message Could not peek recvmsg() mgd connection

Description The web management process could not peek the incoming MGD request.

Type Error: An error occurred

Severity error

WEB_MGD_SOCKET_ERROR

System Log Message Could not create mgd listener socket

Description The web management process could not open the MGD listening socket.

Type Error: An error occurred

Severity error

WEB_PIDFILE_LOCK

System Log Message Unable to lock PID file *pathname*: *error-message*

Description The Web management gatekeeper process (httpd-gk) attempted to lock the indicated file, which records its process ID (PID). The file serves to prevent multiple instances of httpd-gk from running simultaneously. The attempt failed for the indicated reason.

Type Error: An error occurred

Severity error

WEB_PIDFILE_UPDATE

System Log Message Unable to update PID file *pathname*: *error-message*

Description The Web management gatekeeper process (httpd-gk) attempted to update the indicated file, which records the process ID (PID) of the running httpd-gk process. The file serves to prevent multiple instances of httpd-gk from running simultaneously. The attempt failed for the indicated reason.

Type Error: An error occurred

Severity error

Cause The most common reason is that another httpd-gk process was already running.

WEB_UNAME_FAILED

System Log Message Unable to retrieve system hostname: *error-message*

Description The Web management gatekeeper process (httpd-gk) attempted to retrieve and store the local hostname, which it shares with its remote clients. The attempt failed for the indicated reason.

Type Error: An error occurred

Severity error

WEB_WEBAUTH_AUTH_FAIL

System Log Message Web-authentication of user *username* with fwauthd failed

Description The web-authentication authentication process was unable to authenticate the indicated user

Type Event: This message reports an event, not an error

Severity notice

WEB_WEBAUTH_AUTH_OK

System Log Message Web-authentication of user *username* with fwauthd successful

Description The web-authentication authentication process was able to authenticate the indicated user successfully

Type Event: This message reports an event, not an error

Severity notice

WEB_WEBAUTH_CONNECT_FAIL

System Log Message Unable to connect to fwauthd on socket *file-descriptor*: *error-message*

Description The web-authentication authentication process could not connect to fwauthd daemon on the indicated socket

Type Event: This message reports an event, not an error

Severity error

Part 3
Index

Index

Symbols

A

B

C

U

V

W