

Logging System Events

11

The ERX system allows you to log system events to discover and isolate problems with your system. This chapter shows how to use the CLI to monitor your system's log configuration and stay abreast of all system events that you want to track.

Topic	Page
Overview	11-1
Configuring Event Logging	11-3
Monitoring Logging System Events	11-12
List of Event Categories	11-16

Overview

System events are classified into event categories. Using the CLI, you can determine which event categories to log. To take the most advantage of the logging facility, it is important to understand the terms *log severity* and *log verbosity*.

Log Severity

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

The minimum severity of a log message for an individual category is described either by a severity number in the range 0–7 or a descriptive priority term, such as *emergency* or *debug*. The lower the severity number is, the higher the priority. See Table 11-1.



Note: *Not every event category supports every severity level. For a list of event categories and the severity levels that each category supports, see List of Event Categories later in this chapter.*

Table 11-1 Log severity descriptions

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

Log Verbosity

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

- Low – terse
- Medium – moderate
- High – verbose



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

Persistent Logs

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

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

Configuring Event Logging

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

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

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

- Set the log severity.

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

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

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

- Set the log verbosity.

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

- Log messages to a specified destination.

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

- Select fields to be added to logs.

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

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

```
host1#log here
```

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

baseline log

- Use to set a baseline for logging events. Only log messages timestamped after the baseline will appear when you enter the **show log data delta** command.
- To use the current system time, do not enter any options.
- To set a specific time, use the following syntax:
Hour:Minute[:Second] – current time in 24-hour format. Seconds are optional.
- **utc** – enter this keyword to indicate that the time entered is in universal coordinated time (UTC), rather than local time.
- To set a specific date, use the following syntax:
Month Day Year – you must spell out the name of the month.

- **last-reset** – causes the system to display log messages generated since the last time the system was reset
- Examples

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

- There is no **no** version.

log destination



- Use to log messages to the specified destination, including system log, console, and nv-file (nonvolatile storage).
 - Note:** *You can display traffic logs—such as ipTraffic, icmpTraffic, tcpTraffic, and udpTraffic—only via the **show log data** command or from the SRP module console. You cannot redirect traffic logs elsewhere, such as to a system log or nonvolatile storage file, or to a Telnet session.*
- Use the **severity** keyword to limit the messages logged based on priority level.
- The following information applies to logging messages to system log servers.
 - › You can have multiple system log servers, but must configure logging to each one separately.
 - › A particular message within a specified event category is logged to a particular system log server only if the priority of the message is greater than or equal to both the priority of the event category and the priority of that system log server.
 - › If you log messages to a system log server, you can also specify:
 - **facility** – specifies a facility ID on the system log destination host. The range is 0–7, representing the logging facilities local0–local7.
 - **include** – logs only the listed categories to system log; no other categories are logged unless specifically included by issuing this command again.
 - **exclude** – logs all categories to system log except the listed categories; all other categories are logged unless specifically excluded by issuing this command again.
 - › Issuing an **include** command after an **exclude** command (or vice versa) overrides the earlier command. Therefore, you cannot enter a command including certain categories and then follow it with a command excluding others. Similarly, you cannot enter a command excluding certain categories and then follow it with a command including others.
 - › You can issue successive **include** commands or successive **exclude** commands; in this case, the successive commands expand the list of included or excluded categories.
- In this example, the first command causes *only* the ospfGeneral, mplsGeneral, and os event categories to be logged to system log at 10.10.9.5. The second command reverses this inclusion and restores the logging of *all* event categories.

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

host1(config)#no log destination syslog 10.10.9.5
```

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

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

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

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

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

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

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

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

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

- In this example, the first command causes the isisGeneral event category to be excluded from logging to system log at 10.1.2.3. The second command causes ospfGeneral to also be excluded from logging.

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

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

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

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

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

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

log destination syslog source

- Use to specify a source interface type and location for events logged to system log at the specified IP address.
- Overrides the actual source interface type and location. The IP address associated with the specified source interface will be used as the source address for subsequent system log messages.
- Example

```
host1(config)#log destination syslog 10.1.2.3 source atm 0/1
```
- Use the **no** version to restore the actual source interface type and location.

log engineering

- Use to enable engineering logs.
- This command can provide you with troubleshooting information that will assist you when contacting Juniper Networks Customer Service.
- Example

```
host1(config)#log engineering
```
- Use the **no** form of this command to disable engineering logs.

log fields

- Use to select fields to be added to all logs. These fields include a timestamp for the message, an instance identifier, and the name of the internal software application that created the message.
- Example

```
host1(config)#log fields timestamp instance no-calling-task
```
- Use the **no** version to restore the default log field settings.

log here

- Use to enable logs destined for a console to be displayed at the current console.
- By default, the local console automatically receives all log messages if console is a destination. The exception is the cliCommand log. These log events do not appear on the console.
- By default, Telnet consoles do not receive log messages.
- Example

```
host1#log here
```
- Use the **no** version to disable logs destined for a console from being displayed on this console.

log severity

- Use to set the severity level for a selected category or for systemwide logs. For a list of severity values, see Table 11-1.
- If you do not specify a category, then the severity value is set for all categories, except individual logs for which you previously set a specific value. See the next section, *Configuring Log Severity for Individual and Systemwide Logs*.
- Each event category has its own default severity value. For most categories, the default is error.
- To disable log messages use the **off** keyword.
- Example

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

- Use the **no** version to return to the default severity value (error) for the selected category. To return all logs to their default severity setting, include an * (asterisk) with the **no** version. For example:

```
host1(config)#no log severity *
```

log unlimit

- Use to remove the limit on the number of outstanding buffers for an event category. You would remove the limit in cases where the system is dropping logs of a particular category.
- Example

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

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

log verbosity

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

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

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

Configuring Log Severity for Individual and Systemwide Logs

Each event category has its own default severity setting that is based on the type of log messages for that category. You can change the severity setting for *individual* logs and the *systemwide* value:

- To change the log severity of an individual log, set the individual log category to an explicit value. The new value overrides any systemwide value, and subsequent commands that set the systemwide severity value do not override the value you set for the individual log. To return an individual log severity to its default value, which also allows the

individual log severity to be overridden by the systemwide value, use the **no** version of the **log severity** command, and specify the individual log category.

- To change the log severity of every log, set the systemwide severity. The systemwide severity setting does not override individual log severities that you explicitly set.
- To return all logs, systemwide and individual, to their default severity level, use the **no log severity *** command.

Examples The following example sets all logs to log at severity info, except for the bgpEvents and bgpRoutes categories.

```
host1(config)#log severity warning bgpEvents
host1(config)#log severity notice bgpRoutes
host1(config)#log severity info
```

The following command removes the severity values for bgpEvents; bgpEvents now logs at the info severity level.

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

The following command returns all logs to their default severity level.

```
host1(config)#no log severity *
```

To see whether individual or systemwide severity and verbosity settings are in effect, use the **show log configuration** command.

Configuring Log Verbosity for Individual Logs or All Logs

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

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

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

Setting the Timestamp for Log Messages

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

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

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

```
host1(config)#clock timezone EDT -5
host1(config)#service timestamps log datetime show-timezone
localtime
host1#exit
host1#show log data category cliCommand severity info
*****
NOTICE 05/14/2001 13:22:48 EDT cliCommand: "clock timezone
EDT -5", console
NOTICE 05/14/2001 13:23:03 EDT cliCommand: "service
timestamps log datetime show-timezone localtime ", console
*****
```

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

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

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

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

```
NOTICE 05/14/2001 18:28:42 UTC EDT cliCommand: "service
timestamps log datetime show-timezone", console
*****
```

- Display no timestamp on the log messages.

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

service timestamps

- Use to format timestamps for log messages.
- For information about setting local times and time zones, see *Chapter 9, Configuring the System Clock*
- The **show log data** command displays the log data with the current timestamp format.
- The **show log data nv-file** command displays the log data with the timestamp format in effect at the time the log record was written.
- Use the **no** version to remove timestamps from log messages.

Configuring Log Filters

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

You define filters when you set the log severity for an event category. The online Help shows the options you can set for each filter. The following example creates a filter that logs BGP connection information at the debug severity level on traffic that matches access list ListOne, and is incoming traffic to virtual router default.

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

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

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

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

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

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

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

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

List of Event Categories, later in this chapter, includes the filters available in each event category.

Turning Off Filters

There are three ways to turn off filters. The first turns off all filters, the second lets you turn off all filters for an event category, and the third lets you turn off a specific filter.

To turn off all filters:

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

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

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

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

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

no log filters

- Use to turn off log filters.
- To turn off all filters for an event category, specify the category name.
- To turn off a specific filter, use the **no** version of the **log severity** command that you used to add the filter.
- Example

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

Monitoring Logging System Events

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

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

show log configuration

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

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

category	severity	verbosity	filters
NameResolverLog	ERROR	low	
aaaAtml483Cfg	ERROR	low	

```

aaaEngineGeneral      ERROR      low
aaaServerGeneral     ERROR      low
addressServerGeneral  ERROR      low
atm                   ERROR      low
atm1483               ERROR      low
atmAal5               ERROR      low
bgpConnections       ERROR      low
...
cliCommand            NOTICE    low
controlNetworkSlave  ERROR      low
cops                  ERROR      low
...
udpTraffic            ERROR      low

```

- Example 2 – individual log **udpTraffic** is set to warning

```

host1#(config)#log severity warning udpTraffic

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

```

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

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

- Example 3 – **log severity** is set to alert

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

```
host1#show log configuration
```

```
log destination console severity WARNING
log destination nv-file severity CRITICAL
no log engineering
log fields timestamp instance no-calling-task
log severity ALERT
```

category	severity	verbosity	filters
NameResolverLog	ALERT#	low	
aaaAtm1483Cfg	ALERT#	low	
aaaEngineGeneral	ALERT#	low	
aaaServerGeneral	ALERT#	low	
addressServerGeneral	ALERT#	low	
atm	ALERT#	low	
atm1483	ALERT#	low	
atmAal5	ALERT#	low	
bgpConnections	ALERT#	low	
...			
cliCommand	ALERT#	low	
controlNetworkSlave	ALERT#	low	
cops	ALERT#	low	
...			
udpTraffic	ALERT#	low	

```
# Default severity setting is overridden by the system-wide severity setting.
```

- Example 4 – individual log **atm** is set to severity warning

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

```
host1#show log configuration
```

```
log destination console severity WARNING
log destination nv-file severity CRITICAL
no log engineering
log fields timestamp instance no-calling-task
log severity ALERT
```

category	severity	verbosity	filters
NameResolverLog	ALERT#	low	
aaaAtm1483Cfg	ALERT#	low	
aaaEngineGeneral	ALERT#	low	
aaaServerGeneral	ALERT#	low	
addressServerGeneral	ALERT#	low	
atm	WARNING*	low	

```

atm1483                ALERT#    low
atmAal5                ALERT#    low
bgpConnections         ALERT#    low
...
cliCommand             ALERT#    low
controlNetworkSlave   ALERT#    low
cops                   ALERT#    low
...
udpTraffic             ALERT#    low

```

```

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

```

show log data

- Use to display system events. The following keywords allow you to be selective about which events are displayed.
- **category** – limits the display to a single log event category. Refer to the CLI online Help for available categories.

› Example

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

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

› Example

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

```
logFile.temp: The system cannot find the file specified.
```

```
ALERT 09/12/2000 21:29:17 os: ASSERTION FAILED: file mplSvcs2.cc, line 789
```

```
ALERT 09/20/2000 02:18:06 os: ASSERTION FAILED: file osPool.cc, line 819
```

```
ALERT 09/20/2000 02:26:35 os: ASSERTION FAILED: file osPool.cc, line 819
```

```
ALERT 09/20/2000 02:44:33 os: ASSERTION FAILED: file osPool.cc, line 819
```

```
ALERT 09/20/2000 04:56:35 os: ASSERTION FAILED: file osPool.cc, line 819
```

```
ALERT 09/27/2000 03:10:25 os: ASSERTION FAILED: file
```

```
/sw0/sc/nvs/include/./nvMapBackend.h, line 235
```

```
ALERT 10/02/2000 04:05:42 os: ASSERTION FAILED: file osHeap.cc, line 439
```

```
ALERT 10/02/2000 04:08:04 os: ASSERTION FAILED: file osMessageQueue.cc,
line
```

```
42, ripl
```

```
ALERT 10/12/2000 03:43:38 os: PANIC: file osSemaphore.cc, line 54
```

```
ALERT 11/01/2000 02:03:49 os: ASSERTION FAILED: file cliCommand.cc, line
195
```

- **severity** – displays events that have a specific severity level.

› Example

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

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

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

List of Event Categories

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

aaaAtm1483Cfg

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

aaaEngineGeneral

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

aaaServerGeneral

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

aaaUserAccess

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

addressServerGeneral

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

ar1AaaServerGeneral

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

atm

Description:	ATM interface
Emergency:	None
Alert:	None
Critical:	None
Error:	Unable to reenable ILMI administrative state after UNI version change
Warning:	Error getting location of underlying physical interface; error binding or unbinding to physical interface; error allocating memory for new interface; error setting system identifier; error adding or configuring an interface; error getting capabilities of interface; error getting maximum VPI/VCI for interface; error getting maximum virtual circuit descriptor for interface; unable to store or allocate memory for F4 OAM circuit data; unable to configure F4 OAM circuit for interface
Notice:	Interface pool expanded by an incremental number of entries; report retry delay in seconds when waiting for the underlying physical interface to be created; unable to allocate a message to send an interface up or down notification; unable to add or configure interface
Info:	Dropping interface up, down, or not present notification due to removal of interface; discarding F4 OAM circuits when interface does not support F4 OAM
Debug:	None
Filter:	None

atm1483

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

Info: Dropping subinterface up or down notification due to removal of subinterface; configure interfaces on ATM interface; elapsed time for downloading interfaces; elapsed time for ATM AAL5 present notification; maximum interface count per call; SVC up or down state change

Debug: None

Filter: None

atmAal5

Description: ATM adaptation layer 5

Emergency: None

Alert: None

Critical: None

Error: None

Warning: Error getting location of underlying ATM interface; error binding to ATM interface; unable to expand interface pool; error creating interface; unable to set administrative status of interface

Notice: Interface pool expanded by an incremental number of entries; report retry delay in seconds when waiting for the underlying ATM interface to be created; unable to allocate a message to send an interface up or down notification

Info: Dropping interface up or down notification due to removal of interface

Debug: None

Filter: None

AuditIpsec

Description: IKE SA negotiations

Emergency: None

Alert: None

Critical: None

Error: None

Warning: None

Notice: Information on IKE SA negotiation payloads

Info: None

Debug: None

Filter: None

bgpConnections

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

bgpDampening

Description:	BGP dampening
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	Route is suppressed by route-flap dampening; route is no longer suppressed by route-flap dampening
Info:	None
Debug:	None

- Filter 1:** access-class – this filter is not currently supported
- Filter 2:** peer – see description of the bgpRoutes peer filter for information on this filter
- Filter 3:** route-map – this filter is not currently supported
- Filter 4:** router – see description of the bgpRoutes router filter for information on this filter
- Filter 5:** in – this filter is not currently supported
- Filter 6:** out – this filter is not currently supported

bgpEvents

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

bgpGeneral

Description:	BGP general information
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	None
Debug:	None
Filter 1:	access-class – this filter is not currently supported
Filter 2:	peer – see description of the bgpRoutes peer filter for information on this filter
Filter 3:	route-map –this filter is not currently supported
Filter 4:	router – see description of the bgpRoutes router filter for information on this filter
Filter 5:	in – this filter is not currently supported
Filter 6:	out – this filter is not currently supported

bgpKeepAlives


Description:	BGP keepalive messages
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	Keepalive message received with unexpected additional data after header
Notice:	Keepalive message received; keepalive message sent
Info:	None
Debug:	None
Filter 1:	access-class – this filter is not currently supported
Filter 2:	peer – see description of the bgpRoutes peer filter for information on this filter
Filter 3:	route-map – this filter is not currently supported
Filter 4:	router – see description of the bgpRoutes router filter for information on this filter

- Filter 5:** in – matches on traffic coming into the router
- Filter 6:** out – matches on traffic going out of the router



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

bgpMessages

- Description:** BGP protocol messages
 - Emergency:** None
 - Alert:** None
 - Critical:** None
 - Error:** None
 - Warning:** Unknown message type received; invalid field in received message; notification message received or sent^a; invalid capability length in received ORF capability; invalid capability value in received ORF capability; invalid ORF in received ORF capability; ORF entries exceeded maximum limit in received prefix list
 - Notice:** Open message received or sent^a; update message received or sent; route-refresh message received or sent^a; route-refresh-cisco message received or sent^a; received ORF capability; received route refresh message with ORF entries
 - Info:** None
 - Debug:** Keepalive message received or sent^a
-  **Note:** Send messages are logged to the *bgpMessages* log when a message is added to the send queue. A debug message is logged to the *bgpConnections* log when the message is actually passed to TCP.
- Filter 1:** access-class – this filter is not currently supported
 - Filter 2:** peer – see description of the *bgpRoutes* peer filter for information on this filter
 - Filter 3:** route-map – this filter is not currently supported
 - Filter 4:** router – see description of the *bgpRoutes* router filter for information on this filter
 - Filter 5:** in – matches on traffic coming into the router
 - Filter 6:** out – matches on traffic going out of the router

a. Full decode of message logged if verbosity is high.

bgpNeighborChanges

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

bgpRoutes

Description:	BGP routing table updates
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	Failure to add, remove, or modify BGP route in IP forwarding table
Notice:	BGP route added to, removed from, or modified in the IP forwarding table; aggregate route added to, removed from, or modified in Loc-RIB; network route added to, removed from, or modified in Loc-RIB; best route for internal peers for a given prefix became available; best route for internal peers for a given prefix is no longer available, has changed, or has become available; best route for external peers for a given prefix is no longer available, has changed, or has become available; MPLS base tunnel used to reach an indirect next-hop came up or went down; MPLS stacked tunnel for label came up; indirect next-hop became reachable or unreachable; direct next-hop for an indirect next-hop changed
Info:	None

Debug: Redistributed route added to, removed from, or modified in Loc-RIB; advertisement for a given prefix received; withdraw for a given prefix received

Filter 1: `access-class accessClassName [route-map routeMapName routeMapOptions | filtering-router filteringRouterName filteringRouterOptions | in | out]`

- `access-class` – log events for traffic that matches a specific access class
- `accessClassName` – name of the access class for which you want to log events
- `route-map` – log events for traffic that matches a specific route map
- `routeMapName` – name of route map for which you want to log events
- `routeMapOptions` – in the following format – filtering-router `filteringRouterName filteringRouterOptions | in | out`
- `filtering-router` – log events only if the access class or route map are defined on a specific virtual router
- `filteringRouterName` – virtual router where the access class and/or route map are defined
- `filteringRouterOptions` – in | out
- `in` – matches on traffic coming into the access class, route map, or virtual router
- `out` – matches on traffic sent out of the access class, route map, or virtual router

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

- `peer` – log events for traffic that matches a specific peer
- `peerIpAddress` – address of the peer for which you want to log events
- `access-class` – log events for traffic that matches a specific access class
- `accessClassName` – name of the access class for which you want to log events
- `accessClassOptions` – in the following format – filtering-router `filteringRouterName filteringRouterOptions | in | out`
- `route-map` – log events for traffic that matches a specific route map
- `routeMapName` – name of route map for which you want to log events
- `routeMapOptions` – in the following format – filtering-router `filteringRouterName filteringRouterOptions | in | out`
- `filtering-router` – log events only if the peer, access class or route map are defined on a specific virtual router
- `filteringRouterName` – virtual router where the peer, access class and/or route map are defined
- `filteringRouterOptions` – in | out
- `in` – matches on traffic coming into the peer, access class, route map, or virtual router
- `out` – matches on traffic sent out of the peer, access class, route map, or virtual router

- Filter 3:** `route-map routeMapName [filtering-router filteringRouterName filteringRouterOptions | in | out]`
- `route-map` – log events for traffic that matches a specific route map
 - `routeMapName` – name of route map for which you want to log events
 - `filtering-router` – log events only if the route map is defined on a specific virtual router
 - `filteringRouterName` – virtual router where the route map is defined
 - `filteringRouterOptions` – in | out
 - `in` – matches on traffic coming into the route map or virtual router
 - `out` – matches on traffic sent out of the route map or virtual router
- Filter 4:** `router virtualRouterName [access-class accessClassName accessClassOptions | route-map routeMapName routeMapOptions | filtering-router filteringRouterName filteringRouterOptions | peer peerIpAddress peerOptions | in | out]`
- `router` – log events for traffic on a specific virtual router
 - `virtual-router-name` – name of virtual router
 - `access-class` – log events for traffic that matches a specific access class on the specified router
 - `accessClassName` – name of the access class for which you want to log events
 - `accessClassOptions` – in the following format – `route-map routeMapName routeMapOptions | virtual-router virtualRouterName virtualRouterOptions | in | out`
 - `route-map` – log events for traffic that matches a specific route map
 - `routeMapName` – name of route map for which you want to log events
 - `routeMapOptions` – in the following format – `virtual-router virtualRouterName virtualRouterOptions | in | out`
 - `filtering-router` – log events only if the access class or route map is defined on a specific virtual router
 - `filteringRouterName` – virtual router where the access class or route map is defined
 - `filteringRouterOptions` – in the following format – in | out
 - `peer` – log events for traffic that matches a specific peer
 - `peerIpAddress` – address of the peer for which you want to log events
 - `peerOptions` – in the following format – `access-class accessClassName accessClassOptions | filtering-router filteringRouterName filteringRouterOptions | route-map routeMapName routeMapOptions | in | out`
 - `in` – matches on traffic coming into the virtual router, access class, or route map
 - `out` – matches on traffic sent out of the virtual router, access class, or route map
- Filter 5:** `in` – matches on traffic coming into the router
- Filter 6:** `out` – matches on traffic going out of the router

bgpVpn

Description:	BGP VPN
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	None
Debug:	None
Filter 1:	access-class – this filter is not currently supported
Filter 2:	peer – this filter is not currently supported
Filter 3:	route-map – this filter is not currently supported
Filter 4:	router – this filter is not currently supported
Filter 5:	in – this filter is not currently supported
Filter 6:	out – this filter is not currently supported

bridgedEthernet

Description:	Bridged Ethernet protocol layer
Emergency:	None
Alert:	None
Critical:	Out of resources
Error:	Mismatch in configuration or NVRAM
Warning:	None
Notice:	Removing interface from NVRAM
Info:	Hardware state change
Debug:	None
Filter:	None

bulkStats

Description:	Bulk statistics collector
Emergency:	None
Alert:	None
Critical:	None
Error:	None

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

cacGeneral

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

cacIntf

Description:	CAC interface events
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	Unusual or failure situations in interface processing
Notice:	None
Info:	None
Debug:	Interface level debugging info
Filter:	interface <i>interfaceType interfaceSpecifier</i>

- *interfaceType* – type of interface on which you want to log events
- *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

cbf

Description:	General connection-based forwarding
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	Error creating, modifying, or removing an interface or connection; error saving or storing a configuration
Notice:	Interface or connection created, modified, or removed
Info:	Change in interface status, location, or location availability
Debug:	Configuration saved or restored
Filter:	None

cliCommand

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

cops

Description:	Common Open Policy Service (COPS) protocol
Emergency:	None
Alert:	None
Critical:	None
Error:	COPS message with bad header, version, length, or client
Warning:	Unexpected socket event
Notice:	COPS layer enabled or disabled; socket remotely closed

Info:	None
Debug:	COPS session instantiation or removal; COPS connection or socket creation or deletion; keepalive value
Filter:	None

crl dpGeneral

Description:	Constraint-based Routed Label Distribution Protocol (CRLDP) general
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	Sessions not being connected; memory allocation failures; internal protocol failures; protocol message processing failures
Notice:	Configuration problems; resource shortfalls; memory allocation failures when processing configuration directives; invalid protocol messages received; LSP loops detected; session or adjacency errors
Info:	Minor protocol message processing errors; minor configuration problems
Debug:	None
Filter:	<pre>router <i>virtualRouterName</i> {trace <i>traceOptions</i>}</pre> <ul style="list-style-type: none">• <code>router</code> – log events for traffic on a specific virtual router• <code><i>virtualRouterName</i></code> – name of virtual router for which you want to log events• <code>trace</code> – you can optionally trace specific types of activity• <code><i>traceOptions</i></code> – type(s) of activity to trace. You can trace any of the following types of activity, and you can trace multiple types of activity by including multiple trace options in the command. For example, the following command causes configuration changes, function calls, and performance to be traced. <pre>host1(config)#log severity info crldpgeneral router westford trace config func perf</pre> <ul style="list-style-type: none">› <code>config</code> – configuration changes› <code>crutil</code> – CRLDP subsystem› <code>demux</code> – demultiplexer activity› <code>flow</code> – data flows› <code>func</code> – function calls› <code>hello</code> – hello traffic› <code>init</code> – initialization activity› <code>input</code> – input activity› <code>Imm</code> – Imm activity› <code>smif</code> – label space manager interfaces› <code>nmadap</code> – network management adaptation layer› <code>notf</code> – notification activity

- › output – output activity
- › perf – performance
- › reif – routing entity interface activity
- › sciif – switch controller interface activity
- › sessions – session activity
- › teif – traffic engineering interface activity
- › util – utility subsystems

ctreeLog

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

dcm

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

dcmEngineGeneral

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

dhcpGeneral

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

dhcpLocalServerGeneral

Description:	General DHCP local server
Emergency:	None
Alert:	None
Critical:	None
Error:	Memory allocation failure
Warning:	Invalid configuration; DHCP packet drops due to invalid local server state or resource exhaustion; address limit violations; SDX communication problems; invalid DHCP packets
Notice:	Authentication denial

Info: None

Debug: Receive packet; transmit packet; authentication status; DHCP local pool resolution; address allocation; DHCP local server state transition; NVS actions; configuration changes

dhcpNvGeneral

Description: DHCP host route preservation

Emergency: None

Alert: None

Critical: None

Error: Null interface for DHCP clients

Warning: None

Notice: None

Info: Output from VxWorks shell “dhcp-NvShow” command

Debug: NVS cache creation; entries added to or removed from the cache; cache synchronized to NVS

Filter: None

dhcpRelayGeneral

Description: DHCP Relay general

Emergency: None

Alert: None

Critical: None

Error: None

Warning: None

Notice: None

Info: None

Debug: Control flow and key events

Filter: None

dhcpProxyGeneral

Description: DHCP Proxy general

Emergency: None

Alert: None

Critical: None

Error: None

Warning:	None
Notice:	None
Info:	None
Debug:	Control flow and key events
Filter:	None

diagMboxCtrl

Description:	Power-on-self-test (POST) is run via CLI on console
Emergency:	None
Alert:	None
Critical:	None
Error:	PPC7XX to PPC860 mailbox not functioning
Warning:	PPC860 processor does not boot
Notice:	None
Info:	None
Debug:	PPC860 test execution time
Filter:	None

dnsGeneralLog

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

ds1

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

ds3

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

dvmrpGeneral

Description:	DVMRP general
Emergency:	None
Alert:	None
Critical:	None
Error:	Memory allocation errors; bad parameters (internal errors); designated forwarder (DF) errors (two for same interface, DoNotForward by no DF);

processing prune errors; graft errors; internal errors; catastrophic RT table errors; management interaction errors; NVS errors

- Warning:** Unable to add local route; routeHogCheck; routeLimit
- Notice:** Route expiration; pruneProcessing (send or receive); graftAck processing; source group (SG) state information; deletion of an output interface (OIF); nbrQuickDelete; nbrReset; nbrTimeOut; error adding neighbor on Route Report Reception
- Info:** DF election information; sending graft; timer expired for MulticastEntry; attempting to log duplicate accept filter; external route deleted or added
- Debug:** Local address creation or deletion; information about accept filters; dvmrpInterface creation or deletion; sgTimeout information; noMoreOifs info; sg creation information; multicastForwarding enabled or disabled; DvmrpInit; dvmrpEnable/Disable; rpfCallback
- Filter 1:** interface *interfaceType interfaceSpecifier*
- interface – log events for a specific interface
 - *interfaceType* – type of interface for which you want to log events
 - *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see ERX Command Reference Guide, About This Guide.

- Filter 2:** router *virtualRouterName* [interface *interfaceType interfaceSpecifier*]
- router – log events for a specific virtual router
 - *virtualRouterName* – name of virtual router for which you want to log events
 - interface – log events on a specific interface on the virtual router
 - *interfaceType* – type of interface for which you want to log events
 - *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see ERX Command Reference Guide, About This Guide.

dvmrpMcastTable

-
- Description:** DVMRP multicast table messages
- Emergency:** None
- Alert:** None
- Critical:** None
- Error:** Error removing MulticastEntry; adding duplicate MulticastEntry; adding nonexistent MulticastEntry; attempting to send prune to nonexistent neighbor; error deleting MulticastEntry; error adding OIF
- Warning:** Deleting MulticastEntry with no SG state found; attempting to create MulticastEntry, but unable to do so
- Notice:** Creating MulticastEntry
- Info:** rePruning; delOif; add OIF; not adding OIF for some reason; creating sgofflist; pruneDelayCallback; prune; deleting MulticastEntry

Debug:	None
Filter 1:	interface – see description of the dvmrpGeneral interface filter for information on this filter
Filter 2:	router – see description of the dvmrpGeneral router filter for information on this filter

dvmrpProbeRcv

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

dvmrpProbeSent

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

dvmrpRtTable

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

ethernet

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

fileSystem

Description:	File system
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	Missing of invalid armed files

Notice:	None
Info:	None
Debug:	Timestamp of last synchronization
Filter:	None

frameRelay

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

fsAgent

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

ft1

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

ftpClient

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

ftpServer

Description:	FTP server
Emergency:	None
Alert:	None
Critical:	None
Error:	Error listening for new client connection; error creating daemon task
Warning:	Error creating new server task; socket write error; error adjusting socket window size

Notice:	Daemon task created; waiting for new client connection; accept client from host a.b.c.d; maximum client sessions exceeded; FTP daemon shutdown complete
Info:	Starting FTP daemon shutdown
Debug:	Read FTP command

gplaan

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

httpServer

Description:	Embedded HTTP server
Emergency:	None
Alert:	None
Critical:	None
Error:	Failure to enable HTTP daemons (httpd); failure to remove httpd; failure to grow pool of httpds; failure to listen on httpd socket; unable to create or remove session with DHCP Local Server (dhcp-ls); failure to grow pool of HTTP connections (httpcs); failure to set TCP socket options; failure to remove TCP socket; failure to queue HTTP event (socket accept, socket approve, socket send, socket receive); failure to queue HTTP event for maximum connection aging; failure to queue HTTP event for dhcp-ls (newaddress, gplaanAdd, gplaanRemove); failure to find session to dhcp-ls; received invalid token address from dhcp-ls; out of resources for adding new address at dhcp-ls session; invalid http event
Warning:	Refused HTTP connection due to too many simultaneous connections from same host; refused HTTP connection due to access list deny; failure to perform TCP socket approval; failure to send data on TCP socket; unexpected token address from DHCP-LS session; authentication failure from dhcp-ls for a given client
Notice:	None

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

icmpTraffic

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

igmpGeneral

Description:	IGMP general
Emergency:	None
Alert:	None
Critical:	None
Error:	Nonrecoverable errors
Warning:	NVS errors
Notice:	Errors while configuring or learning groups
Info:	None
Debug:	IGMP interface or group state change; errors in packet transmit or receive
Filter 1:	interface <i>interfaceType interfaceSpecifier</i>

- interface – log events for a specific interface
- *interfaceType* – type of interface for which you want to log events
- *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

Filter 2:	router <i>virtualRouterName</i> [interface <i>interfaceType interfaceSpecifier</i>]
------------------	---

- router – log events for a specific virtual router
- *virtualRouterName* – name of virtual router for which you want to log events
- interface – log events on a specific interface on the virtual router
- *interfaceType* – type of interface for which you want to log events
- *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

ikepki

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

Debug:	Detailed SA negotiation debug information
Filter:	Filter

ipAccessList



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

ipEngine

Description:	IP chassis manager
Emergency:	None
Alert:	None
Critical:	None
Error:	Failure in operations such as adding, removing, or deleting interfaces or distributing routing tables to line modules
Warning:	Errors such as attempting to configure something that is not supported on a module, or routing table memory is approaching 80% full

- Notice:** Something unexpected happened; for example, an interface was deleted twice or, internal to the software, connections between IC and SRP were deleted twice
- Info:** Completion status of a user command (for example: "IS command succeeded")
- Debug:** An engine or agent that corresponds to a virtual router is added or deleted; an interface is added or deleted

ipGeneral

- Description:** IP general
- Emergency:** None
- Alert:** None
- Critical:** (IP) Interface stacking management errors
- Error:** (ARP) Allocation of Ethernet next hop failed
- (IP) Not able to create interface or create address on null 0 interface; undefined IP status code; interface stacking management errors; send and forward failures because of not finding corresponding egress or ingress nodes; conflict in adding hidden routes
- Warning:** (IP) NVS load errors; failure to add address on an interface because of low memory
- Notice:** None
- Info:** None
- Debug:** (ARP) NextHopPool is out of memory and trying to expire old entries; ARP data events
(IP) Interface stacking management errors
- Filter 1:** interface *interfaceType interfaceSpecifier*
- interface – log events for a specific interface
 - *interfaceType* – type of interface for which you want to log events
 - *interfaceSpecifier* – location of interface in the appropriate format
-  **Note:** For information on interface types and specifiers, see ERX Command Reference Guide, About This Guide.
- Filter 2:** router *virtualRouterName [interface interfaceType interfaceSpecifier]*
- router – log events for a specific virtual router
 - *virtualRouterName* – name of virtual router for which you want to log events
 - interface – log events on a specific interface on the virtual router
 - *interfaceType* – type of interface for which you want to log events. For example, atm or fastEthernet.
 - *interfaceSpecifier* – location of interface in the appropriate format
-  **Note:** For information on interface types and specifiers, see ERX Command Reference Guide, About This Guide.

ipInterface

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

ipNhopTrackerGeneral

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

ipProfileMgr

Description:	IP Profile Manager
Emergency:	None
Alert:	None
Critical:	None
Error:	Failure to create or delete dynamic IP interfaces
Warning:	None

Notice:	None
Info:	None
Debug:	Events related to dynamic IP interface creation or deletion; assignment or unassignment of profiles to interfaces
Filter:	None

ipRoutePolicy

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

ipRouteTable

Description:	IP routing table
Emergency:	None
Alert:	None
Critical:	None
Error:	Next-hop resolution-related problems
Warning:	Failure to add route
Notice:	None
Info:	In process of finding best route information
Debug:	Normal routing table updates; next-hop resolution for static routes
Filter 1:	interface – see description of the ipGeneral interface filter for information on this filter
Filter 2:	router – see description of the ipGeneral router filter on information on this filter

ipTraffic

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

ipTunnel

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

isisAdjChange

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

Debug: None

Filter 1: interface *interfaceType* *interfaceSpecifier*

- interface – log events for a specific interface
- *interfaceType* – type of interface for which you want to log events
- *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

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

- router – log events for a specific virtual router
- *virtualRouterName* – name of virtual router for which you want to log events
- interface – log events on a specific interface on the virtual router
- *interfaceType* – type of interface for which you want to log events
- *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

isisAdjPackets

Description: IS-IS adjacency hello packets

Emergency: None

Alert: None

Critical: None

Error: None

Warning: Error in sent IIH or received IIH

Notice: Sent or received IIH, DR election

Info: Authentication failed

Debug: Detailed information about IIH

Filter 1: interface – see description of the isisAdjChange interface filter for information on this filter

Filter 2: router – see description of the isisAdjChange router filter for information on this filter

isisChecksumErr

Description: IS-IS checksum errors

Emergency: None

Alert: None

Critical: None

Error: None

Warning:	LSP checksum error
Notice:	None
Info:	None
Debug:	None
Filter 1:	interface – see description of the isisAdjChange interface filter for information on this filter
Filter 2:	router – see description of the isisAdjChange router filter for information on this filter

isisGeneral

Description:	IS-IS system notifications
Emergency:	None
Alert:	None
Critical:	None
Error:	Error in restoring NVS
Warning:	Exceeding maximum IP addresses on interface or maximum sequence number
Notice:	Error in redistributing routes; LAN circuit coming up
Info:	None
Debug:	Redistributed routes
Filter 1:	interface – see description of the isisAdjChange interface filter for information on this filter
Filter 2:	router – see description of the isisAdjChange router filter for information on this filter

isisLocalUpdate

Description:	IS-IS local LSP packets
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	Sent local LSP
Info:	None
Debug:	None

- Filter 1:** interface – see description of the isisAdjChange interface filter for information on this filter
- Filter 2:** router – see description of the isisAdjChange router filter for information on this filter

isisMplsTeAdvertisements

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

isisMplsTeEvents

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

isisProtocolErr

Description:	IS-IS protocol errors
Emergency:	None
Alert:	None
Critical:	None
Error:	None

Warning:	LSP protocol error
Notice:	None
Info:	None
Debug:	None
Filter:	router <i>virtualRouterName</i> <ul style="list-style-type: none">• router – log events for a specific virtual router• <i>virtualRouterName</i> – name of virtual router for which you want to log events

isisSnpPackets

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

isisSpfEvents

Description:	IS-IS Shortest Path First (SPF)
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	Start or suspend SPF; updating routing table
Info:	Add tent or path; process LSP

Debug: Add route
Filter: router *virtualRouterName*

- router – log events for a specific virtual router
- *virtualRouterName* – name of virtual router for which you want to log events

isisSpfStatistics

Description: IS-IS SPF timing and statistic data
Emergency: None
Alert: None
Critical: None
Error: None
Warning: None
Notice: SPF compute time
Info: None
Debug: None
Filter: router *virtualRouterName*

- router – log events for a specific virtual router
- *virtualRouterName* – name of virtual router for which you want to log events

isisSpfTriggers

Description: IS-IS SPF triggering
Emergency: None
Alert: None
Critical: None
Error: None
Warning: None
Notice: SPF trigger event
Info: None
Debug: None
Filter: router *virtualRouterName*

- router – log events for a specific virtual router
- *virtualRouterName* – name of virtual router for which you want to log events

isisUpdatePackets

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

l2f

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

l2fIpLowerBinding

Description:	Layer 2 Forwarding over IP
Emergency:	None
Alert:	None
Critical:	None
Error:	Recoverable error
Warning:	Protocol error; insufficient resources
Notice:	None
Info:	None

Debug: Function trace
Filter: None

l2fStateMachine

Description: Layer 2 Forwarding state machine trace
Emergency: None
Alert: None
Critical: None
Error: None
Warning: Unexpected state machine transitions
Notice: None
Info: State machine trace
Debug: State machine timer operations
Filter: None

l2tp

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

l2tpIpLowerBinding

Description: Layer 2 Tunneling Protocol over IP
Emergency: None
Alert: None
Critical: None
Error: Recoverable error
Warning: Protocol error; insufficient resources
Notice: None

Info:	None
Debug:	None
Filter:	None

l2tpStateMachine

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

localAddressServerGeneral



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

localLinePassword

Description:	Local line password authentication server
Emergency:	None
Alert:	None
Critical:	None
Error:	Unknown algorithm for local password

Warning:	Connection granted or denied due to possible misconfiguration
Notice:	None
Info:	None
Debug:	Connection granted or denied due to incorrect password
Filter:	None

mgtmGeneral

Description:	Mgtm general information
Emergency:	None
Alert:	None
Critical:	None
Error:	Major errors in MGMTM API calls resulting in failure
Warning:	IP Multicast fastpath forwarding not supported on interface
Notice:	Errors in MGMTM API calls
Info:	State change events; invalid parameters in API calls
Debug:	<Source, Group> entries not found
Filter 1:	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> • interface – log events for a specific interface • <i>interfaceType</i> – type of interface for which you want to log events • <i>interfaceSpecifier</i> – location of interface in the appropriate format <p>Note: For information on interface types and specifiers, see <i>ERX Command Reference Guide, About This Guide</i>.</p>
 Filter 2:	router <i>virtualRouterName</i> [interface <i>interfaceType</i> <i>interfaceSpecifier</i>] <ul style="list-style-type: none"> • router – log events for a specific virtual router • <i>virtualRouterName</i> – name of virtual router for which you want to log events • interface – log events on a specific interface on the virtual router • <i>interfaceType</i> – type of interface for which you want to log events • <i>interfaceSpecifier</i> – location of interface in the appropriate format <p>Note: For information on interface types and specifiers, see <i>ERX Command Reference Guide, About This Guide</i>.</p>
	

mmcd

Description:	MMC switch fabric driver
Emergency:	None
Alert:	None
Critical:	None

Error:	Errors in hardware configuration; resource limitation in fabric reached; errors in hardware
Warning:	None
Notice:	None
Info:	None
Debug:	Initialization details; configuration details; connection status details
Filter:	None

mplsAppService

Description:	MPLS application service
Emergency:	None
Alert:	None
Critical:	LSM platform label space creation failure; tunnel information access failure
Error:	Upper interface stacking or unstacking interaction failures; global tunnel information; storage failures; MPLS engine failures
Warning:	None
Notice:	None
Info:	Upper stacking information
Debug:	Upper interface stacking or unstacking transactions; global MPLS engine transactions; global tunnel information storage transactions; LSM platform label space transactions
Filter:	None

mplsGeneral

Description:	MPLS general purpose
Emergency:	None
Alert:	None
Critical:	Resource allocation failures; initialization failures; fatal internal errors
Error:	Signaling protocol errors; nonfatal internal errors; configuration errors
Warning:	Signaling protocol configuration problems; major interface deletion; minor internal errors; CRLDP session status
Notice:	None
Info:	NVS operations
Debug:	NVS operations; timer operations; minor interface label stacking; function flows

- Filter:** router *virtualRouterName*
- router – log events for a specific virtual router
 - *virtualRouterName* – name of virtual router for which you want to log events

mplsMajorInterface


- Description:** MPLS major interface
- Emergency:** None
- Alert:** None
- Critical:** None
- Error:** Signaling protocol interaction failures; major interface engine interaction failures; major interface finite state machine bad state transitions; major interface configuration errors; LSM interface label space interaction failures
- Warning:** None
- Notice:** None
- Info:** None
- Debug:** Major interface finite state machine transitions; signaling protocol interaction; major interface to engine transactions; major interface configuration transactions; LSM interface label space transactions
- Filter:** router *virtualRouterName* [interface *interfaceType* *interfaceSpecifier*]
- router – log events for a specific virtual router
 - *virtualRouterName* – name of virtual router for which you want to log events
 - interface – log events on a specific interface on the virtual router
 - *interfaceType* – type of interface for which you want to log events
 - *interfaceSpecifier* – location of interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

mplsMinorInterface

- Description:** MPLS minor interface
- Emergency:** None
- Alert:** None
- Critical:** None
- Error:** Tunnel/LSP setup or teardown signaling protocol interaction failures; minor interface engine interaction failures; minor interface finite state machine bad state transitions; minor interface configuration errors; minor interface to IP interaction failures
- Warning:** None

Notice:	None
Info:	None
Debug:	Minor interface to engine transactions; minor interface to IP transactions; minor interface configuration transactions; signaling protocol LSP setup or teardown transactions; minor interface finite state machine transitions
Filter 1:	interface <i>interfaceType</i> <i>interfaceSpecifier</i> <ul style="list-style-type: none"> • interface – log events for a specific interface • <i>interfaceType</i> – type of interface for which you want to log events • <i>interfaceSpecifier</i> – location of interface in the appropriate format  <p>Note: For information on interface types and specifiers, see <i>ERX Command Reference Guide, About This Guide</i>.</p>
Filter 2:	router <i>virtualRouterName</i> <ul style="list-style-type: none"> • router – log events for a specific virtual router • <i>virtualRouterName</i> – name of virtual router for which you want to log events

mtraceLog

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

mtracercvdLog

Description:	mtrace packets received
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	Short description of the received mtrace packets

Debug: Complete print of the received mtrace packets
Filter: None

mtraceSentLog

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

multicastTraffic

Description: IP multicast frame transmit or receive
Emergency: None
Alert: None
Critical: None
Error: None
Warning: None
Notice: None
Info: None
Debug: IP multicast packet transmit or receive information
Filter 1: remote-ip-address *ipAddress* [*ipAddressMask*]

- remote-ip-address – log events for a remote address
- *ipAddress* – address of remote system for which you want to log messages
- *ipAddressMask* – mask for the remote address

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

- router – log events on a specific virtual router
- *virtualRouterName* – name of virtual router for which you want to log events

- `remote-ip-address` – log events for a remote address
- `ipAddress` – address of remote system for which you want to log messages
- `ipAddressMask` – mask for the remote address

nameResolverLog

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

noneAaaAddrServer

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

noneAaaServer

Description:	Authentication and accounting client
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None

Info: None
Debug: Notification of automatic success response to authentication or accounting request
Filter: None

ntpGeneral

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

onlineDiag

Description: Online diagnostics for tests run in the background
Emergency: None
Alert: None
Critical: None
Error: Any errors detected during tests
Warning: The PPC860 processor does not boot
Notice: Names of tests being run during onlineDiags; memory sizes detected
Info: Fabric connections; memory sizes
Debug: Very verbose messages for debugging errors and register accesses
Filter: None

OS

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

ospfElectDr

Description:	OSPF designated router (DR) election
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	DR election events
Info:	None
Debug:	None

Filter 1: `interface-ip-address [ip-address ipAddress | unnumbered interfaceType interfaceSpecifier]`

- `interface-ip-address` – log events for a specific interface
- `ip-address` – specifies that you will identify the interface by entering an IP address
- `ipAddress` – IP address of interface for which you want to log events
- `unnumbered` – specifies that the interface is unnumbered
- `interfaceType` – to identify unnumbered interface, enter type of interface for which you want to log events
- `interfaceSpecifier` – location of the unnumbered interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

Filter 2: `router virtualRouterName [interface-ip-address [ip-address ipAddress | unnumbered interfaceType interfaceSpecifier]]`

- `router` – log events for a specific virtual router
- `virtualRouterName` – name of virtual router for which you want to log events
- `interface-ip-address` – log events for a specific interface on the virtual router
- `ip-address` – specifies that you will identify the interface by entering an IP address
- `ipAddress` – IP address of interface for which you want to log events
- `unnumbered` – specifies that the interface is unnumbered
- `interfaceType` – to identify the unnumbered interface, enter the type of interface for which you want to log events
- `interfaceSpecifier` – location of the unnumbered interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

ospfGeneral

Description:	OSPF general
Emergency:	None
Alert:	None
Critical:	None
Error:	Error enabling or disabling OSPF; allocation errors
Warning:	State change errors (for example, OSPF could not be enabled); errors creating or destroying an area, an OSPF range, or a virtual link
Notice:	OSPF enabled or disabled
Info:	None
Debug:	None

Filter 1:	interface-ip-address – see description of the ospfElectDr interface filter for information on this filter
Filter 2:	router – see description of the ospfElectDr router filter for information on this filter

ospfInterface

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

ospfLsa

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

- Filter 2:** router *virtualRouterName* [neighbor *neighborIpAddress*]
- router – log events on a specific virtual router
 - *virtualRouterName* – virtual router on which you want to log events
 - neighbor – log events associated with a specific neighbor
 - *neighborIpAddress* – IP address of neighbor for which you want to log events

ospfNeighbor

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

ospfPktsRcvd

- Description:** OSPF packet received
- Emergency:** None
- Alert:** None
- Critical:** None
- Error:** None
- Warning:** Packets discarded; validation errors
- Notice:** Number of LSAs packed in different packet types (LSA Ack, LSA update); packets received over Down interface
- Info:** None
- Debug:** Packets received description

Filter 1:	interface-ip-address – see description of the ospfElectDr interface filter for information on this filter
Filter 2:	router – see description of the ospfElectDr router filter for information on this filter

ospfPktsSent

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

ospfRoute

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

ospfSpfExt

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

ospfSpfInter

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

ospfSpfIntra

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

ospfTeDatabase

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

ospfTeSPF

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

pimAutoRPRcvdLog

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



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

- Filter 2:** router *virtualRouterName* [interface-ip-address [ip-address *ipAddress* | unnumbered *interfaceType interfaceSpecifier*]]
- router – log events for a specific virtual router
 - *virtualRouterName* – name of virtual router for which you want to log events
 - interface-ip-address – log events for a specific interface on the virtual router
 - ip-address – specifies that you will identify the interface by entering an IP address
 - *ipAddress* – IP address of interface for which you want to log events
 - unnumbered – specifies that the interface is unnumbered
 - *interfaceType* – to identify unnumbered interface, enter type of interface for which you want to log events
 - *interfaceSpecifier* – location of unnumbered interface in the appropriate format



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

pimAutoRPSentLog

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

pimHelloRcvdLog

Description:	Protocol Independent Multicast (PIM) Hello messages received
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None

Notice:	None
Info:	Short description of the received PIM hello messages
Debug:	Complete printout of the received PIM hello messages
Filter 1:	interface-ip-address – see description of the pimAutoRPRcvdLog interface-ip-address filter for information on this filter
Filter 2:	router – see description of the pimAutoRPRcvdLog router filter for information on this filter

pimHelloSentLog

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

pimPktsRcvdLog

Description:	Protocol Independent Multicast (PIM) nonhello (Register/RegisterStop/JoinPrune/Assert/Graft/GraftAck) messages received
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	Short description of the PIM messages received
Debug:	Complete description of the PIM messages received

- Filter 1:** interface-ip-address – see description of the pimAutoRPRcvdLog interface-ip-address filter for information on this filter
- Filter 2:** router – see description of the pimAutoRPRcvdLog router filter for information on this filter

pimPktsSentLog

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

policyMgrAttachment

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

policyMgrGeneral


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

policyMgrPacketLog


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

ppp

Description:	Point-to-Point Protocol layer
Emergency:	None
Alert:	None
Critical:	Nonrecoverable error
Error:	Recoverable error
Warning:	Resource or configuration problem
Notice:	Authentication actions
Info:	None
Debug:	Detailed debugging information

Filter:	interface <i>interfaceType</i> <i>interfaceIdentifier</i>
	<ul style="list-style-type: none"> • interface – logs PPP events for a specific interface • <i>interfaceType</i> – type of interface for which you want to log PPP events • <i>interfaceIdentifier</i> – location of interface in the appropriate format
	Note: For information on interface types and specifiers, see <i>ERX Command Reference Guide, About This Guide</i> .

pppoe


Description:	Point-to-Point over Ethernet layer
Emergency:	None
Alert:	None
Critical:	None
Error:	Error enabling control packet log
Warning:	PPPoE interface or subInterface removed from NVS
Notice:	PPPoE enabled; status change for subInterface
Info:	Line module status change
Debug:	None
Filter:	interface <i>interfaceType</i> <i>interfaceSpecifier</i>
	<ul style="list-style-type: none"> • interface – logs PPP events for a specific interface • <i>interfaceType</i> – type of interface for which you want to log PPP events • <i>interfaceSpecifier</i> – location of interface in the appropriate format
	Note: For information on interface types and specifiers, see <i>ERX Command Reference Guide, About This Guide</i> .

pppoeControlPacket

Description:	PPPoE control packet trace
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	None
Debug:	Control packets logged; control packet log enabled

Filter: interface *interfaceType* *interfaceSpecifier*

- interface – logs PPP events for a specific interface
- *interfaceType* – type of interface for which you want to log PPP events
- *interfaceSpecifier* – location of interface in the appropriate format

 **Note:** For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

pppPacket

Description: PPP packet capture

Emergency: None

Alert: None

Critical: None

Error: None

Warning: None


Notice: None

Info: None

Debug: Packet trace

Filter: interface *interfaceType* *interfaceSpecifier*

- interface – logs PPP events for a specific interface
- *interfaceType* – type of interface for which you want to log PPP events
- *interfaceSpecifier* – location of interface in the appropriate format

 **Note:** For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

pppStateMachine

Description: PPP state machine trace

Emergency: None

Alert: None

Critical: None


Error: None

Warning: None

Notice: None

Info: None

Debug: State machine trace

Filter:	interface <i>interfaceType</i> <i>interfaceSpecifier</i>
	<ul style="list-style-type: none"> • interface – logs PPP events for a specific interface • <i>interfaceType</i> – type of interface for which you want to log PPP events. For example, atm or fastEthernet • <i>interfaceSpecifier</i> – location of interface in the appropriate format
	Note: For information on interface types and specifiers, see <i>ERX Command Reference Guide, About This Guide</i> .

profileMgr

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

qos

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

radiusAttributes

Description:	RADIUS User Attributes
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	None
Debug:	Supported RADIUS attributes found in the Access-Accept or Access-Reject packet
Filter:	None

radiusClient

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

remOps

Description:	Remote operations
Emergency:	None
Alert:	None
Critical:	None
Error:	Internal error
Warning:	Maximum table size reached; ICMP failure; same target probed by more than one entry

Notice:	Remote operations application begin/start; ping, traceroute, or nslookup entry; create, modify, or remove; unexpected packet receive; invalid target or source address; late packet receive
Debug:	Ping, traceroute, or nslookup session begin or end; packet receive; duplicate receive
Filter:	None

ripGeneral

Description:	RIP system notifications
Emergency:	None
Alert:	None
Critical:	None
Error:	Failed to redistribute an external route to the RIP; failed to establish peer with neighbor due to the memory limitation; general RIP configuration error, such as an access list name or route map name specified in the RIP config mode exceed maximum allowable length
Warning:	Failed to process a RIP packet due to the current memory limitation
Notice:	Enable or disable RIP application
Info:	None
Debug:	RIP query; RIP peer address
Filter 1:	interface <i>interfaceType interfaceSpecifier</i> <ul style="list-style-type: none">• <i>interface</i> – logs PPP events for a specific interface• <i>interfaceType</i> – type of interface for which you want to log events• <i>interfaceSpecifier</i> – location of interface in the appropriate format
Filter 2:	router <i>virtualRouterName</i> <ul style="list-style-type: none">• <i>router</i> – log events for a specific virtual router• <i>virtualRouterName</i> – name of virtual router for which you want to log events

ripRoute

Description:	RIP route
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	None

- Debug:** Routes sent or received by RIP; if a route is rejected or not sent, gives the reason
- Filter 1:** `interface interfaceType interfaceSpecifier`
- `interface` – logs PPP events for a specific interface
 - `interfaceType` – type of interface for which you want to log events
 - `interfaceSpecifier` – location of interface in the appropriate format
- Filter 2:** `router virtualRouterName`
- `router` – log events for a specific virtual router
 - `virtualRouterName` – name of virtual router for which you want to log events

ripRtTable

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

routerLog

- Description:** Virtual router log
- Emergency:** None
- Alert:** None
- Critical:** None
- Error:** None
- Warning:** None
- Notice:** Creation and deletion of virtual routers
- Info:** None
- Debug:** None
- Filter:** `router virtualRouterName`
- `router` – log events for a specific virtual router

security

Description:	CLI security messages
Emergency:	None
Alert:	None
Critical:	Suspected denial of service attack
Error:	None
Warning:	Unrecognized username, invalid password, denied host
Notice:	User connect, user disconnect
Info:	None
Debug:	None
Filter:	None

slep

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



Note: For information on interface types and specifiers, see *ERX Command Reference Guide, About This Guide*.

snmp

Description:	Embedded SNMP agent
Emergency:	None
Alert:	None
Critical:	None
Error:	None

Warning:	Access violation due to underprivileged community string or a bad proxy selector; access denial due to configured access list; configuration of SNMP failed; trap is dropped because of the severity level filter or because the trap category is not enabled
Notice:	None
Info:	SNMP agent has been enabled or disabled
Debug:	Trap request dropped; trap processing summary statistics
Filter:	None

snmpPduAudit

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

snmpSetPduAudit

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

sonet

Description:	SONET
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	NV interface removal after failed init from NV; errors during interface add/update or during hwPresent notification; path capability notification; failed pool expansion
Notice:	Pool expansion
Info:	NV interface creation; interface modification from path capability; unknown interface during hwNotPresent notification; interface notification for unknown interface
Debug:	None
Filter:	None

sonetPath

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

sonetVT

Description:	SONET virtual tributary
Emergency:	None
Alert:	None
Critical:	None

Error:	None
Warning:	Init from NV failures; errors during remove interface; failed pool expansion
Notice:	Engine add interface retry; pool expansion
Info:	Errors during add interface
Debug:	None
Filter:	None

ssccDetailPm

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

ssccDetailSc

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

ssccGeneral

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

stTunnel

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

system

Description:	System management and monitoring
Emergency:	None
Alert:	None
Critical:	Line module ping failure threshold exceeded
Error:	Critical subsystem failure condition (NVS, power, fan, network timing, temperature); unrecognized module type; module ID mismatch; line

	module memory reduction; line module bandwidth misconfiguration; unrecoverable file system synchronization errors
Warning:	Noncritical subsystem failure condition (heap/CPU utilization, NVS, network timing); unexpected software error; recoverable file system synchronization errors; file system out of synchronization notification; NVS subsystem redundancy size mismatch; line module ID block misconfigured
Notice:	Subsystem failure condition abatement (heap/CPU utilization, NVS, power, fan, network timing, temperature); new module announcement; module revision mismatch; module upgraded or downgraded (ECC/non-ECC); module online or offline
Info:	Synchronization start, complete; line module set timing failed (not necessarily an error); NVS volume flush
Debug:	Module state change; module memory announcement; redundancy role changes; server role changes; module enable, disable, or clear notification; file system synchronization (normal operation); line module timing source set failure (not necessarily an error); image protection notification
Filter:	slot <i>slotNumber</i> <ul style="list-style-type: none"> • slot – log events for a specific slot • <i>slotNumber</i> – number of slot for which you want to log events

tcpGeneral

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

tcpTraffic

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

telnet

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

testExec

Description:	Test executive when POST is run via CLI on console
Emergency:	None
Alert:	None
Critical:	None
Error:	Errors detected during POST
Warning:	The PPC860 processor does not boot
Notice:	Names of tests being executed during POST, memory sizes detected
Info:	FPGA image CRCs; fabric connections; redundancy information
Debug:	Very verbose messages for debugging errors; FPGA image info; register accesses
Filter:	None

tsm

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

udpTraffic

Description:	UDP frame transmit or receive
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	None
Notice:	None
Info:	None

Debug:	Report all UDP receive or transmit events
Filter 1:	remote-ip-address <i>ipAddress</i> [<i>ipAddressMask</i>] <ul style="list-style-type: none"> remote-ip-address – log events for a remote address <i>ipAddress</i> – address of remote system for which you want to log messages <i>ipAddressMask</i> – optionally supply a mask for the remote address
Filter 2:	router <i>virtualRouterName</i> [remote-ip-address <i>ipAddress</i> [<i>ipAddressMask</i>]] <ul style="list-style-type: none"> router – log events on a specific virtual router <i>virtualRouterName</i> – name of virtual router for which you want to log events remote-ip-address – log events for a remote address <i>ipAddress</i> – address of remote system for which you want to log messages <i>ipAddressMask</i> – optionally supply a mask for the remote address

vrfVpnMgrGeneralLog

Description:	VPN routing and forwarding (VRF) VPN manager general
Emergency:	None
Alert:	None
Critical:	None
Error:	None
Warning:	Dynamic VPN shared interface creation and deletion failures; duplicate notifications from different sessions to IP
Notice:	None
Info:	None
Debug:	Notifications VrfVpnMgr receives from interface session and other sessions to IP; deletion and creation of dynamic VPN-shared interfaces
Filter:	None

vrrp

Description:	Virtual Router Redundancy Protocol
Emergency:	None
Alert:	None
Critical:	NVS error; out of resources; unexpected error
Error:	Virtual router ID (VRID) creation or modification failure; association addresses creation or modification failure
Warning:	IP interface used by VRRP was removed; unexpected advertisement received from neighbor; invalid authentication detected; unable to get IP interface's primary address

Notice: VRRP neighbor found

Info: State machine change

Debug: Management get, set, create, and remove

Filter: *interfaceType interfaceSpecifier [vrrpIdentifier]*

- *interfaceType* – type of interface for which you want to log events
- *interfaceSpecifier* – location of interface in the appropriate format
- *vrrpIdentifier* – ID of the VRRP router for which you want to log events



Note: *For information on interface types and specifiers, see ERX Command Reference Guide, About This Guide.*