Chapter 1

System Logging Overview

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

This chapter contains the following sections:

Overview of System Logging

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

Log Severity

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

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

NOTE: Not every event category supports every severity level. For a list of event categories and the severity levels that each category supports, see *Chapter 2, Event Categories*.

Table 4: Log Severity Descriptions

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

Log Verbosity

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

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

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

Persistent Logs

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

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

Logging Platform Considerations

System logs are supported on all E-series routers.

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

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

Configuring Event Logging

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

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

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

- Set the log severity.

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

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

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

- Set the log verbosity.

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

- Log messages to a specified destination.

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

- Select fields to be added to logs.

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

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

  host1#**log here**

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

baseline log

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

- To set a specific time, use the following syntax:

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

- **utc**—Enter this keyword to indicate that the time entered is in universal coordinated time (UTC), rather than local time.

- To set a specific date, use the following syntax:

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

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

- Examples

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

- There is no **no** version.

log destination

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

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

- Use the **severity** keyword to limit the messages logged based on priority level.

- The following information applies to logging messages to system log servers.

  - You can have multiple system log servers, but must configure logging to each one separately.

  - A particular message within a specified event category is logged to a particular system log server only if the priority of the message is greater than or equal to both the priority of the event category and the priority of that system log server.

  - If you log messages to a system log server, you can also specify:

    - **facility**—Specifies a facility ID on the system log destination host. The range is 0–7, representing the logging facilities local0–local7.

    - **include**—Logs only the listed categories to system log; no other categories are logged unless specifically included by issuing this command again.

- **exclude**—Logs all categories to system log except the listed categories; all other categories are logged unless specifically excluded by issuing this command again.

- Issuing an **include** command after an **exclude** command (or vice versa) overrides the earlier command. Therefore, you cannot enter a command including certain categories and then follow it with a command excluding others. Similarly, you cannot enter a command excluding certain categories and then follow it with a command including others.

- You can issue successive **include** commands or successive **exclude** commands; in this case, the successive commands expand the list of included or excluded categories.

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

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

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

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

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

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

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

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

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

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

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

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

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

log destination syslog source

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

  host1(config)#**log destination syslog 10.1.2.3 source atm 0/1**

- Use the **no** version to restore the actual source interface type and location.

log engineering

- Use to enable engineering logs.
- Provides troubleshooting information to assist you when contacting Juniper Networks Technical Assistance Center (JTAC).
- Example

  host1(config)#**log engineering**

- Use the **no** form of this command to disable engineering logs.

log fields

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

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

- Use the **no** version to restore the default log field settings.

log here

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

  host1#**log here**

- Use the **no** version to disable logs destined for a console from being displayed on this console.

log severity

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

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

- If you do not specify a category, the severity value changes for all categories except individual categories for which you previously set a specific severity level. See *Configuring Log Severity for Individual and Systemwide Logs* on page 8 for details.
- Each event category has its own default severity value. For most categories, the default is Error.
- To disable all *default* level log messages, use the **off** keyword without specifying an event category.
- To disable individual level log messages, use the **off** keyword and specify the event category that you want to disable.
- Example

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

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

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

log unlimit

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

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

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

log verbosity

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

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

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

Configuring Log Severity for Individual and Systemwide Logs

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

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

- All log event categories have a default. However, the default values can vary for each category. For example, most event categories have a default severity of Error. However, some event categories may have a default severity of Notice, Warning, Info, and so on.
- Log event categories have two states—unassigned (default) and assigned. How a log event category reacts to the **log severity** command depends on its current state.
- You can change log severities for event categories at a systemwide level or an individual level. Systemwide changes are those that modify a large number of unassigned event categories at one time; for example, the command **log severity debug off**. Individual changes are those that indicate an explicit event category that you want to change; for example, the command **log severity notice clicommand**.
- Changes to log event categories at an individual level take precedence over those made at the systemwide level.
- Changes to log event categories at the systemwide level take precedence over the default.

- Assigning a log severity to an individual event category changes its state to Assigned. This means that you cannot change the severity of that event category using systemwide level commands until you return the event category to its default, unassigned state by using the **no log severity** *eventCategory* command.
- To return all logs, systemwide and individual, to their default, unassigned severity level, use the **no log severity *** command.
- To see whether individual or systemwide severity and verbosity settings are in effect, use the **show log configuration** command.

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

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

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

Warning: Logging to this terminal is disabled
    no log severity

      category         severity   verbosity   filters   notes
--------------------   --------   ---------   -------   -----
aaaAtm1483Cfg          ERROR      low
aaaEngineGeneral       ERROR      low
aaaServerGeneral       ERROR      low
aaaUserAccess          ERROR      low
addressServerGeneral   ERROR      low
ar1AaaServerGeneral    ERROR      low
atm                    ERROR      low
atm1483                ERROR      low
atmAal5                ERROR      low
```

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

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

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

Warning: Logging to this terminal is disabled
    log severity WARNING
```

```
      category          severity   verbosity   filters   notes
--------------------    --------   ---------   -------   -----
aaaAtm1483Cfg           WARNING    low                   1
aaaEngineGeneral        WARNING    low                   1
aaaServerGeneral        WARNING    low                   1
aaaUserAccess           WARNING    low                   1
addressServerGeneral    WARNING    low                   1
ar1AaaServerGeneral     WARNING    low                   1
atm                     WARNING    low                   1
atm1483                 WARNING    low                   1
atmAal5                 WARNING    low                   1
```

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

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

Warning: Logging to this terminal is disabled
    log severity WARNING

category                severity   verbosity   filters   notes
--------------------    --------   ---------   -------   -----
aaaAtm1483Cfg           WARNING     low                   1
aaaEngineGeneral        WARNING     low                   1
aaaServerGeneral        WARNING     low                   1
aaaUserAccess           WARNING     low                   1
addressServerGeneral    WARNING     low                   1
ar1AaaServerGeneral     WARNING     low                   1
atm                     EMERGENCY   low                   2
atm1483                 WARNING     low                   1
atmAal5                 WARNING     low                   1
```

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

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

Warning: Logging to this terminal is disabled
    log severity ALERT

category                severity   verbosity   filters   notes
--------------------    --------   ---------   -------   -----
aaaAtm1483Cfg           ALERT       low                   1
aaaEngineGeneral        ALERT       low                   1
aaaServerGeneral        ALERT       low                   1
aaaUserAccess           ALERT       low                   1
addressServerGeneral    ALERT       low                   1
ar1AaaServerGeneral     ALERT       low                   1
```

```
atm                    EMERGENCY   low                  2
atm1483                ALERT       low                  1
atmAal5                ALERT       low                  1
```

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

5. Turn off log notification, systemwide, and view the log configuration:

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

Warning: Logging to this terminal is disabled
    log severity OFF

      category         severity    verbosity   filters   notes
--------------------   ---------   ---------   -------   -----
aaaAtm1483Cfg          OFF         low                   1
aaaEngineGeneral       OFF         low                   1
aaaServerGeneral       OFF         low                   1
aaaUserAccess          OFF         low                   1
addressServerGeneral   OFF         low                   1
ar1AaaServerGeneral    OFF         low                   1
atm                    EMERGENCY   low                   2
atm1483                OFF         low                   1
atmAal5                OFF         low                   1
```

Notice that the atm event category does not change.

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

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

Warning: Logging to this terminal is disabled
    log severity OFF

      category         severity   verbosity   filters   notes
--------------------   --------   ---------   -------   -----
aaaAtm1483Cfg          OFF        low                   1
aaaEngineGeneral       OFF        low                   1
aaaServerGeneral       OFF        low                   1
aaaUserAccess          OFF        low                   1
addressServerGeneral   OFF        low                   1
ar1AaaServerGeneral    OFF        low                   1
atm                    OFF        low                   1
atm1483                OFF        low                   1
atmAal5                OFF        low                   1
```

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

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

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

Warning: Logging to this terminal is disabled
    no log severity

      category         severity   verbosity   filters   notes
--------------------   --------   ---------   -------   -----
aaaAtm1483Cfg          ERROR      low
aaaEngineGeneral       ERROR      low
aaaServerGeneral       ERROR      low
aaaUserAccess          ERROR      low
addressServerGeneral   ERROR      low
ar1AaaServerGeneral    ERROR      low
atm                    ERROR      low
atm1483                ERROR      low
atmAal5                ERROR      low
```

Configuring Log Verbosity for Individual Logs or All Logs

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

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

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

Setting the Timestamp for Log Messages

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

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

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

  host1(config)#**clock timezone EDT -5**

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

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

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

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

- Display no timestamp on the log messages.

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

service timestamps

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

Configuring Log Filters

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

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

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

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

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

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

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

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

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

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

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

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

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

Turning Off Log Filters

You can turn off filters in three ways:

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

To turn off all filters:

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

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

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

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

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

no log filters

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

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

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

Monitoring Logging System Events

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

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

show log configuration

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

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

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

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

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

        category            severity   verbosity   filters
-------------------------   --------   ---------   -------
NameResolverLog             ERROR      low
aaaAtm1483Cfg               ERROR      low
aaaEngineGeneral            ERROR      low
aaaServerGeneral            ERROR      low
addressServerGeneral        ERROR      low
atm                         ERROR      low
atm1483                     ERROR      low
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.
- Use keywords to select which events are displayed:
  - **category**—Limits the display to a single log event category. See the CLI online Help for available categories.
    - Example

      host1#**show log data category os**

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

```
host1#show log data nv-file
logFile.temp: The system cannot find the file specified.
ALERT 09/12/2000 21:29:17 os: ASSERTION FAILED: file mplsNvs2.cc, line 789
ALERT 09/20/2000 02:18:06 os: ASSERTION FAILED: file osPool.cc, line 819
ALERT 09/20/2000 02:26:35 os: ASSERTION FAILED: file osPool.cc, line 819
```

```
ALERT 09/20/2000 02:44:33 os: ASSERTION FAILED: file osPool.cc, line 819
ALERT 09/20/2000 04:56:35 os: ASSERTION FAILED: file osPool.cc, line 819
ALERT 09/27/2000 03:10:25 os: ASSERTION FAILED: file
/sw0/sc/nvs/include/../nvMapBackend.h, line 235
ALERT 10/02/2000 04:05:42 os: ASSERTION FAILED: file osHeap.cc, line 439
ALERT 10/02/2000 04:08:04 os: ASSERTION FAILED: file osMessageQueue.cc, line
42, rip1
ALERT 10/12/2000 03:43:38 os: PANIC: file osSemaphore.cc, line 54
ALERT 11/01/2000 02:03:49 os: ASSERTION FAILED: file cliCommand.cc, line 195
```

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

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

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

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