Chapter 22

Track Normal Operations

This chapter describes how to configure system logging to monitor system-wide, high-level operations. (See Table 48.)

Table 48: Checklist for Tracking Normal Operations

Track Normal Operations Tasks	Command or Action
Configure System Logging on page 263	
1. Log Messages to a Local Log File on page 263	[edit] [edit system syslog] set file *filename facility level* show commit
2. Log Information to a Remote Host on page 265	[edit] [edit system syslog] set host *hostname facility level* show commit
3. Log Information to a User Terminal on page 266	[edit] [edit system syslog] set user *username facility level* show commit
4. Log Information to a Router Console on page 267	[edit] [edit system syslog] set console *facility level* show commit
5. Configure the Number and Size of Log Files on page 267	[edit] [edit system syslog] set archive files *number* size *size* show commit or [edit] [edit system syslog file *filename]* set archive files *number* size *size* show commit

Track Normal Operations Tasks	Command or Action
6. Log BGP State Transition Events on page 268	[edit] [edit protocol bgp] set log-updown show commit
7. Display a Log File on page 270	show log *filename*
8. Monitor Messages in Near-Real Time on page 271	monitor start *filename*
9. Stop Monitoring Log Files on page 271	monitor stop *filename* or monitor stop

Configure System Logging

Purpose System logging operations use a system logging mechanism to record system-wide, high-level operations, such as interfaces going up or down and users logging in to or out of a router.

Steps To Take To configure system logging, follow these steps:

1. Log Messages to a Local Log File on page 263
2. Log Information to a Remote Host on page 265
3. Log Information to a User Terminal on page 266
4. Log Information to a Router Console on page 267
5. Configure the Number and Size of Log Files on page 267
6. Log BGP State Transition Events on page 268
7. Display a Log File on page 270
8. Monitor Messages in Near-Real Time on page 271
9. Stop Monitoring Log Files on page 271

Step 1: Log Messages to a Local Log File

Action To log messages to a local log file on the router, follow these steps:

1. In configuration mode, go to the following hierarchy level:

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

2. Configure the file, facility, and level:

   ```
   user@host# set file filename facility level
   ```

   For example:

   ```
   [edit system syslog]
   user@host# set file security authorization info
   ```

3. Verify the configuration:

```
user@host# show
```

For example:

```
[edit system syslog]
user@host# show
file security
authorization info
```

4. Commit the configuration:

```
user@host# commit
```

Table 49 lists the JUNOS system logging facilities. Each message is assigned to a facility, which is a group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts).

Table 49: JUNOS System Logging Facilities

Facility	Type of Event or Error
any	Any (includes messages from all facilities).
authorization	Authentication and authorization attempts.
change-log	Change to the JUNOS configuration.
conflict-log	Configuration that is inconsistent with router hardware.
cron	Actions performed or errors encountered by the cron process.
daemon	Actions performed or errors encountered by various system processes.
firewall	Packet filtering actions performed by a firewall filter.
interactive-commands	Commands issued at the JUNOS command-line interface (CLI) operational mode prompt.
kernel	Actions performed or errors encountered by the JUNOS kernel.
pfe	Actions performed or errors encountered by the Packet Forwarding Engine.
user	Actions performed or errors encountered by various user-space processes.

Table 50 lists the system log message severity levels supported by the JUNOS software. Each message is assigned a severity level, which indicates how seriously it affects router functioning.

Table 50: System Log Message Severity Levels

Severity Level	Description
emergency	System panic or other condition that causes the router to stop functioning.
alert	Conditions that require immediate correction, such as a corrupted system database.
critical	Critical conditions, such as hard drive errors.
error	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels.
warning	Conditions that warrant monitoring.
notice	Conditions that are not errors but might warrant special handling.
info	Events or nonerror conditions of interest.
debug	Software debugging messages. Specify this level only when directed by a technical support representative.

Step 2: Log Information to a Remote Host

Action To log messages to a remote host, follow these steps:

1. In configuration mode, go to the following hierarchy level:

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

2. Configure the host, facility, and level:

```
user@host# set host hostname facility level
```

For example:

```
[edit system syslog]
user@host# set host junipero.berry.net daemon info
```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit system syslog]
   user@host# show
   host junipero.berry.net
   daemon info;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

See Also For information on logging facilities and severity levels supported by the JUNOS software, see Table 49 on page 264 and Table 50 on page 265.

Step 3: Log Information to a User Terminal

Action To log messages to a user terminal, follow these steps:

1. In configuration mode, go to the following hierarchy level:

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

2. Configure the user, facility, and level:

   ```
   user@host# set user username facility level
   ```

   For example:

   ```
   [edit system syslog]
   user@host# set user alex any critical
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit system syslog]
   user@host# show
   user alex
       any critical
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

See Also For information on logging facilities and security levels supported by the JUNOS software, see Table 49 on page 264 and Table 50 on page 265.

Step 4: Log Information to a Router Console

Action To log messages to a router console, follow these steps:

1. In configuration mode, go to the following hierarchy level:

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

2. Configure the router console, facility, and level:

   ```
   user@host# set console facility level
   ```

   For example:

   ```
   [edit system syslog]
   user@host# set console any error
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit system syslog]
   user@host# show
   console
   any error
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

See Also For information on logging facilities and security levels supported by the JUNOS software, see Table 49 on page 264 and Table 50 on page 265.

Step 5: Configure the Number and Size of Log Files

Purpose By default, the JUNOS logging facility stops writing messages to a log file when the file reaches 128 KB in size. It closes the file and adds a numerical suffix, then opens and directs messages to a new file with the original name. By default, the JUNOS logging facility creates up to 10 files before it begins overwriting the contents of the oldest file.

Action To configure the number and size of the log files, follow these steps:

1. In configuration mode, go to one of the following hierarchy levels:

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

   or

   ```
   [edit]
   user@host# edit system syslog filename
   ```

2. Configure the number and size of the archive files:

   ```
   user@host# set archive files number size size
   ```

   For example:

   ```
   [edit system syslog]
   user@host# set archive files 10 size 65536
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit system syslog]
   user@host# show
   archive size 64k files 10
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

See Also See the *JUNOS System Basics Configuration Guide* for more detailed explanations and examples of log file configurations.

Step 6: Log BGP State Transition Events

Purpose Border Gateway Protocol (BGP) state transitions indicate a network problem and need to be logged and investigated.

Action To log BGP state transition events to the system log, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit protocol bgp
   ```

2. Configure the system log:

   ```
   user@host# set log-updown
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

What It Means Log messages from BGP state transition events are sufficient to diagnose most BGP session problems. Table 51 lists and describes the six states of a BGP session.

Table 51: Six States of a BGP Session

BGP State	Description
Idle	This is the first state of a connection. BGP waits for a start event initiated by an administrator. The start event might be the establishment of a BGP session through router configuration or the resetting of an existing session. After the start event, BGP initializes its resources, resets a connect-retry timer, initiates a TCP transport connection, and starts listening for connections initiated by remote peers. BGP then transitions to a Connect state. If there are errors, BGP falls back to the Idle state.
Connect	BGP waits for the transport protocol connection to complete. If the TCP transport connection is successful, the state transitions to OpenSent. If the transport connection is not successful, the state transitions to Active. If the connect-retry timer has expired, the state remains in the Connect state, the timer is reset, and a transport connection is initiated. With any other event, the state goes back to Idle.
Active	BGP tries to acquire a peer by initiating a transport protocol connection. If it is successful, the state transitions to OpenSent. If the connect-retry timer expires, BGP restarts the connect timer and falls back to the Connect state. BGP continues to listen for a connection that may be initiated from another peer. The state may go back to Idle in case of other events, such as a stop event. In general, a neighbor state flip-flopping between Connect and Active is an indication that there is a problem with the TCP transport connection. Such a problem might be caused by many TCP retransmissions or the inability of a neighbor to reach the IP address of its peer.
OpenSent	BGP receives an open message from its peer. In the OpenSent state, BGP compares its autonomous system (AS) number with the AS number of its peer and recognizes whether the peer belongs to the same AS (internal BGP) or to a different AS (external BGP). The open message is checked for correctness. In case of errors, such as a bad version number of an unacceptable AS, BGP sends an error-notification message and goes back to Idle. For any other errors, such as expiration of the hold timer or a stop event, BGP sends a notification message with the corresponding error code and falls back to the Idle state. If there are no errors, BGP sends keepalive messages and resets the keepalive timer. In this state, the hold time is negotiated. If the hold time is 0, the hold and keepalive timers are not restarted. When a TCP transport disconnect is detected, the state falls back to Active.

BGP State	Description
OpenConfirm	BGP waits for a keepalive or notification message. If a keepalive is received, the state becomes Established, and the neighbor negotiation is complete. If the system receives an update or keepalive message, it restarts the hold timer (assuming that the negotiated hold time is not 0). If a notification message is received, the state falls back to Idle. The system sends periodic keepalive messages at the rate set by the keepalive timer. In case of a transport disconnect notification or in response to a stop event, the state falls back to Idle. In response to other events, the system sends a notification message with a finite state machine (FSM) error code and goes back to Idle.
Established	This is the final state in the neighbor negotiation. In this state, BGP exchanges update packets with its peers and the hold timer is restarted at the receipt of an update or keepalive message when it is not set to zero. If the system receives a notification message, the state falls back to Idle. Update messages are checked for errors, such as missing attributes, duplicate attributes, and so on. If errors are found, a notification is sent to the peer, and the state falls back to Idle. BGP goes back to Idle when the hold timer expires, a disconnect notification is received from the transport protocol, a stop event is received, or in response to any other event.

See Also For more detailed BGP protocol packet information, configure BGP-specific tracing. See "Track Error Conditions" on page 273 for more information.

Step 7: Display a Log File

Action To look at a log or trace file, use the following JUNOS CLI operational mode command:

user@host> **show log** *filename*

Sample Output

```
user@host> show log messages
Sep 10 07:00:00 host newsyslog[7249]: logfile turned over
Sep 10 07:01:49 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1348
Sep 10 07:04:17 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1349
Sep 10 07:06:45 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1350
Sep 10 07:07:53 host login: 2 LOGIN FAILURES FROM 172.24.16.21
Sep 10 07:07:53 host login: 2 LOGIN FAILURES FROM 172.24.16.21, show
configuration | no-more
```

```
Sep 10 07:08:25 host inetd[2785]: /usr/libexec/telnetd[7251]: exit status 0x100
Sep 10 07:09:13 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1351
Sep 10 07:11:41 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1352
Sep 10 07:14:09 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1353
Sep 10 07:16:37 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1354
Sep 10 07:19:05 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1355
Sep 10 07:21:33 host rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor:
```

What It Means The sample output shows the rpd log messages in the messages file for September 10 from 7:00 to 7:21 AM.

NOTE: Local log files are saved in the /var/log directory.

Step 8: Monitor Messages in Near-Real Time

Action To monitor messages in near-real time as they are being written to the log file, use the following JUNOS CLI operational mode command:

user@host> **monitor start** *filename*

Sample Output

```
user@host> monitor start messages
*** messages ***
Sep 10 19:46:30 router rpd[6451]: bgp_listen_accept: Connection attempt from
unconfigured neighbor: 10.0.8.1+1658
```

What It Means The sample output shows the routing protocol log messages in the messages file for September 10.

Step 9: Stop Monitoring Log Files

Action To stop monitoring log files, use the following JUNOS CLI operational mode command:

user@host> **monitor stop** *filename*

or

user@host> **monitor stop**