Chapter 23

Track Error Conditions

This chapter describes how to configure routing protocol daemon tracing, Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS) protocol, and Open Shortest Path First (OSPF) protocol tracing to diagnose error conditions. (See Table 52.)

Table 52: Checklist for Tracking Error Conditions

Track Error Conditions Tasks	Command or Action
Configure Routing Protocol Process Tracing on page 275	
1. Configure Routing Protocol Process Tracing on page 275	[edit] edit routing-options traceoptions set file *filename* size *size* files *number* show commit run show log *filename*
2. Configure Routing Protocol Tracing for a Specific Routing Protocol on page 278	[edit] edit protocol *protocol-name* traceoptions set file *filename* size *size* files *number* show commit run show log *filename*
3. Monitor Trace File Messages Written in Near-Real Time on page 279	monitor start *filename*
4. Stop Trace File Monitoring on page 280	monitor stop *filename*
Configure BGP-Specific Options on page 281	
1. Display Detailed BGP Protocol Information on page 281	[edit] edit protocol bgp traceoptions set flag update detail show commit run show log *filename*
2. Display Sent or Received BGP Packets on page 283	[edit] edit protocol bgp traceoptions set flag update (send | receive) show commit run show log *filename*

Track Error Conditions Tasks	Command or Action
3. Diagnose BGP Session Establishment Problems on page 284	[edit] edit protocol bgp set traceoptions flag open detail show commit run show log *filename*
Configure IS-IS-Specific Options on page 286	
1. Display Detailed IS-IS Protocol Information on page 286	[edit] edit protocol isis traceoptions set flag hello detail show commit run show log *filename*
2. Display Sent or Received IS-IS Protocol Packets on page 289	[edit] edit protocols isis traceoptions set flag hello (send | receive) show commit run show log *filename*
3. Analyze IS-IS-Link State Packets in Detail on page 291	[edit] edit protocols isis traceoptions set flag lsp detail show commit run show log *filename*
Configure OSPF-Specific Options on page 293	
1. Diagnose OSPF Session Establishment Problems on page 293	[edit] edit protocols ospf traceoptions set flag hello detail show commit run show log *filename*
2. Analyze OSPF Link-State Advertisement Packets in Detail on page 297	[edit] edit protocols ospf traceoptions set flag lsa update detail show commit run show log *filename*

Configure Routing Protocol Process Tracing

Purpose Routing protocol process (rpd) tracing tracks all general routing operations and records them in a log file.

Steps To Take To configure routing protocol process (rpd) tracing and monitor trace file messages, follow these steps:

1. Configure Routing Protocol Process Tracing on page 275
2. Configure Routing Protocol Tracing for a Specific Routing Protocol on page 278
3. Monitor Trace File Messages Written in Near-Real Time on page 279
4. Stop Trace File Monitoring on page 280

Step 1: Configure Routing Protocol Process Tracing

Action To configure routing protocol process (rpd) tracing, follow these steps:

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

   ```
   [edit]
   user@host# edit routing-options traceoptions
   ```

2. Configure the file, file size, number, and flags:

   ```
   [edit routing-options traceoptions]
   user@host# set file filename size size files number
   [edit routing-options traceoptions]
   user@host# set flag flag
   ```

   For example:

   ```
   [edit routing-options traceoptions]
   user@host# set file daemonlog size 10240 files 10
   [edit routing-options traceoptions]
   user@host# set flag general
   ```

3. Verify the configuration:

   user@host# **show**

   For example:

   ```
   [edit routing-options traceoptions]
   user@host# show
   file daemonlog size 10k files 10;
   flag general;
   ```

4. Commit the configuration:

   user@host# **commit**

NOTE: Some traceoptions flags generate an extensive amount of information. Tracing can also slow down the operation of routing protocols. Delete the traceoptions configuration if you no longer require it.

5. View the contents of the file containing the detailed messages:

   user@host# **run show log** *filename*

   For example:

   ```
   [edit routing-options traceoptions]
   user@pro4-a# run show log daemonlog
   Sep 17 14:17:31 trace_on: Tracing to "/var/log/daemonlog" started
   Sep 17 14:17:31 Tracing flags enabled: general
   Sep 17 14:17:31 inet_routerid_notify: Router ID: 10.255.245.44
   Sep 17 14:17:31 inet_routerid_notify: No Router ID assigned
   Sep 17 14:17:31 Initializing LSI globals
   Sep 17 14:17:31 LSI initialization complete
   Sep 17 14:17:31 Initializing OSPF instances
   Sep 17 14:17:31 Reinitializing OSPFv2 instance master
   Sep 17 14:17:31 OSPFv2 instance master running
   [...Output truncated...]
   ```

What It Means Table 53 lists tracing flags and example output for JUNOS-supported routing protocol daemon tracing.

Table 53: Routing Protocol Daemon Tracing Flags

Tracing Flag	Description	Example Output
all	All operations	Not available.
general	Normal operations and routing table change	Not available.
normal	Normal operations	Not available.

Tracing Flag	Description	Example Output
policy	Policy operations and actions	Nov 29 22:19:58 export: Dest 10.0.0.0 proto Static Nov 29 22:19:58 policy_match_qual_or: Qualifier proto Sense: 0 Nov 29 22:19:58 policy_match_qual_or: Qualifier proto Sense: 0 Nov 29 22:19:58 export: Dest 10.10.10.0 proto IS-IS
route	Routing table changes	Nov 29 22:23:59 Nov 29 22:23:59 rtlist_walker_job: rt_list walk for RIB inet.0 started with 42 entries Nov 29 22:23:59 rt_flash_update_callback: flash KRT (inet.0) start Nov 29 22:23:59 rt_flash_update_callback: flash KRT (inet.0) done Nov 29 22:23:59 rtlist_walker_job: rt_list walk for inet.0 ended with 42 entries Nov 29 22:23:59 Nov 29 22:23:59 KRT Request: send len 68 v14 seq 0 CHANGE route/user af 2 addr 172.16.0.0 nhop-type unicast nhop 10.10.10.33 Nov 29 22:23:59 KRT Request: send len 68 v14 seq 0 ADD route/user af 2 addr 172.17.0.0 nhop-type unicast nhop 10.10.10.33 Nov 29 22:23:59 KRT Request: send len 68 v14 seq 0 ADD route/user af 2 addr 10.149.3.0 nhop-type unicast nhop 10.10.10.33 Nov 29 22:24:19 trace_on: Tracing to "/var/log/rpdlog" started Nov 29 22:24:19 KRT Request: send len 68 v14 seq 0 DELETE route/user af 2 addr 10.10.218.0 nhop-type unicast nhop 10.10.10.29 Nov 29 22:24:19 RELEASE 10.10.218.0 255.255.255.0 gw 10.10.10.29,10.10.10.33 BGP pref 170/-101 metric so-1/1/0.0,so-1/1/1.0 <Release Delete Int Ext> as 65401 Nov 29 22:24:19 KRT Request: send len 68 v14 seq 0 DELETE route/user af 2 addr 172.18.0.0 nhop-type unicast nhop 10.10.10.33
state	State transitions	Not available.
task	Interface transactions and processing	Nov 29 22:50:04 foreground dispatch running job task_collect for task Scheduler Nov 29 22:50:04 task_collect_job: freeing task MGMT_Listen (DELETED) Nov 29 22:50:04 foreground dispatch completed job task_collect for task Scheduler Nov 29 22:50:04 background dispatch running job rt_static_update for task RT Nov 29 22:50:04 task_job_delete: delete background job rt_static_update for task RT Nov 29 22:50:04 background dispatch completed job rt_static_update for task RT Nov 29 22:50:04 background dispatch running job Flash update for task RT Nov 29 22:50:04 background dispatch returned job Flash update for task RT Nov 29 22:50:04 background dispatch running job Flash update for task RT Nov 29 22:50:04 task_job_delete: delete background job Flash update for task RT Nov 29 22:50:04 background dispatch completed job Flash update for task RT Nov 29 22:50:04 background dispatch running job Flash update for task RT Nov 29 22:50:04 task_job_delete: delete background job Flash update for task RT
timer	Timer usage	Nov 29 22:52:07 task_timer_hiprio_dispatch: ran 1 timer Nov 29 22:52:07 main: running normal priority timer queue Nov 29 22:52:07 main: ran 1 timer Nov 29 22:52:07 task_timer_hiprio_dispatch: running high priority timer queue Nov 29 22:52:07 task_timer_hiprio_dispatch: ran 1 timer Nov 29 22:52:07 main: running normal priority timer queue Nov 29 22:52:07 main: ran 1 timer Nov 29 22:52:07 main: running normal priority timer queue Nov 29 22:52:07 main: ran 2 timers

Step 2: Configure Routing Protocol Tracing for a Specific Routing Protocol

Action To configure routing protocol tracing for a specific routing protocol, follow these steps:

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

   ```
   [edit]
   user@host# edit protocol protocol-name traceoptions
   ```

2. Configure the file, file size, number, and flags:

   ```
   [edit protocols protocol name traceoptions]
   user@host# set file filename size size files number
   [edit protocols protocol name traceoptions]
   user@host# set flag flag
   ```

   For example:

   ```
   [edit protocols ospf traceoptions]
   user@host# set file ospflog size 10240 files 10
   [edit protocols ospf traceoptions]
   user@host# set flag general
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit protocols ospf traceoptions]
   user@host# show
   file ospflog size 10k files 10;
   flag general;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

5. View the contents of the file containing the detailed messages:

   ```
   user@host# run show log filename
   ```

   For example:

   ```
   [edit protocols ospf traceoptions]
   user@pro4-a# run show log ospflog
   Sep 17 14:23:10 trace_on: Tracing to "/var/log/ospflog" started
   Sep 17 14:23:10 rt_flash_update_callback: flash OSPF (inet.0) start
   Sep 17 14:23:10 OSPF:  multicast address 224.0.0.5/32, route ignored
   Sep 17 14:23:10 rt_flash_update_callback: flash OSPF (inet.0) done
   Sep 17 14:23:10 CHANGE   10.255.245.46/32   gw 10.10.208.67  OSPF
   pref 10/0 metric 1/0 fe-0/0/0.0 <Delete Int>
   Sep 17 14:23:10 CHANGE   10.255.245.46/32   gw 10.10.208.67  OSPF
   pref 10/0 metric 1/0 fe-0/0/0.0 <Active Int>
   Sep 17 14:23:10 ADD      10.255.245.46/32   gw 10.10.208.67  OSPF
   ```

```
pref 10/0 metric 1/0 fe-0/0/0.0 <Active Int>
Sep 17 14:23:10 CHANGE   10.255.245.48/32   gw 10.10.208.69  OSPF
pref 10/0 metric 1/0 fe-0/0/0.0 <Delete Int>
Sep 17 14:23:10 CHANGE   10.255.245.48/32   gw 10.10.208.69  OSPF
pref 10/0 metric 1/0 fe-0/0/0.0 <Active Int>
Sep 17 14:23:10 ADD      10.255.245.48/32   gw 10.10.208.69  OSPF
pref 10/0 metric 1/0 fe-0/0/0.0 <Active Int>
Sep 17 14:23:10 rt_close: 4/4 routes proto OSPF
[...Output truncated...]
```

What It Means Table 54 lists standard tracing options that are available globally or that can be applied to specific protocols. You can also configure tracing for a specific BGP peer or peer group. For more information, see the *JUNOS System Basics Configuration Guide*.

Table 54: Standard Trace Options for Routing Protocols

Tracing Flag	Description
all	All operations
general	Normal operations and routing table changes
normal	Normal operations
policy	Policy operations and actions
route	Routing table changes
state	State transitions
task	Interface transactions and processing
timer	Timer usage

Step 3: Monitor Trace File Messages Written in Near-Real Time

Action To monitor messages in near-real time as they are being written to a trace file, use the following JUNOS command-line interface (CLI) operational mode command:

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

Sample Output

```
user@host> monitor start isis

user@host>
*** isis ***
Sep 15 18:32:21 Updating LSP isis5.02-00 in database
Sep 15 18:32:21 Updating L2 LSP isis5.02-00 in TED
Sep 15 18:32:21 Adding a half link from isis5.02 to isis6.00
Sep 15 18:32:21 Adding a half link from isis5.02 to isis5.00
Sep 15 18:32:21 Adding a half link from isis5.02 to isis6.00
Sep 15 18:32:21 Adding a half link from isis5.02 to isis5.00
Sep 15 18:32:21 Scheduling L2 LSP isis5.02-00 sequence 0xd87 on interface fxp2.3
Sep 15 18:32:21 Updating LSP isis5.00-00 in database
Sep 15 18:32:21 Updating L1 LSP isis5.00-00 in TED
Sep 15 18:32:21 Sending L2 LSP isis5.02-00 on interface fxp2.3
Sep 15 18:32:21     sequence 0xd87, checksum 0xc1c8, lifetime 1200
```

Step 4: Stop Trace File Monitoring

Action To stop monitoring a trace file in near-real time, use the following JUNOS CLI operational mode command after you have started monitoring:

monitor stop *filename*

Sample Output

```
user@host> monitor start isis

user@host>
*** isis ***
Sep 15 18:32:21 Updating LSP isis5.02-00 in database
Sep 15 18:32:21 Updating L2 LSP isis5.02-00 in TED
Sep 15 18:32:21 Adding a half link from isis5.02 to isis6.00
Sep 15 18:32:21 Adding a half link from isis5.02 to isis5.00
Sep 15 18:32:21 Adding a half link from isis5.02 to isis6.00
Sep 15 18:32:21 Adding a half link from isis5.02 to isis5.00
Sep 15 18:32:21 Scheduling L2 LSP isis5.02-00 sequence 0xd87 on interface fxp2.3
Sep 15 18:32:21 Updating LSP isis5.00-00 in database
Sep 15 18:32:21 Updating L1 LSP isis5.00-00 in TED
Sep 15 18:32:21 Sending L2 LSP isis5.02-00 on interface fxp2.3
Sep 15 18:32:21     sequence 0xd87, checksum 0xc1c8, lifetime 1200
monitor stop isis

user@host>
```

Configure BGP-Specific Options

Purpose When unexpected events or problems occur, or if you want to diagnose BGP establishment issues, you can view more detailed information by configuring options specific to BGP. You can also configure tracing for a specific BGP peer or peer group. For more information, see the *JUNOS System Basics Configuration Guide*.

Steps To Take

1. Display Detailed BGP Protocol Information on page 281
2. Display Sent or Received BGP Packets on page 283
3. Diagnose BGP Session Establishment Problems on page 284

Step 1: Display Detailed BGP Protocol Information

Action To display BGP protocol information in detail, follow these steps:

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

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

2. Configure the flag to display detailed BGP protocol messages:

   ```
   [edit protocols bgp traceoptions]
   user@host# set flag update detail
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit protocols bgp traceoptions]
   user@host# show
   flag update detail;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

5. View the contents of the file containing the detailed messages:

   user@host# **run show log** *filename*

   For example:

```
[edit protocols bgp traceoptions]
user@pro5-a# run show log bgp
Sep 17 14:47:16 trace_on: Tracing to "/var/log/bgp" started
Sep 17 14:47:17 bgp_read_v4_update: receiving packet(s) from
10.255.245.53 (Internal AS 10458)
Sep 17 14:47:17 BGP RECV 10.255.245.53+179 -> 10.255.245.50+1141
Sep 17 14:47:17 BGP RECV message type 2 (Update) length 128
Sep 17 14:47:17 BGP RECV flags 0x40 code Origin(1): IGP
Sep 17 14:47:17 BGP RECV flags 0x40 code ASPath(2): 2
Sep 17 14:47:17 BGP RECV flags 0x80 code MultiExitDisc(4): 0
Sep 17 14:47:17 BGP RECV flags 0x40 code LocalPref(5): 100
Sep 17 14:47:17 BGP RECV flags 0xc0 code Extended Communities(16):
2:10458:1
[...Output truncated...]
```

What It Means Table 55 lists tracing flags specific to BGP and presents example output for some of the flags. You can also configure tracing for a specific BGP peer or peer group. For more information, see the *JUNOS System Basics Configuration Guide*.

Table 55: BGP Protocol Tracing Flags

Tracing Flags	Description	Example Output
aspath	AS path regular expression operations	Not available.
damping	Damping operations	Nov 28 17:01:12 bgp_damp_change: Change event Nov 28 17:01:12 bgp_dampen: Damping 10.10.1.0 Nov 28 17:01:12 bgp_damp_change: Change event Nov 28 17:01:12 bgp_dampen: Damping 10.10.2.0 Nov 28 17:01:12 bgp_damp_change: Change event Nov 28 17:01:12 bgp_dampen: Damping 10.10.3.0
keepalive	BGP keepalive messages	Nov 28 17:09:27 bgp_send: sending 19 bytes to 10.217.5.101 (External AS 65471) Nov 28 17:09:27 Nov 28 17:09:27 BGP SEND 10.217.5.1+179 -> 10.217.5.101+52162 Nov 28 17:09:27 BGP SEND message type 4 (KeepAlive) length 19 Nov 28 17:09:28 Nov 28 17:09:28 BGP RECV 10.217.5.101+52162 -> 10.217.5.1+179 Nov 28 17:09:28 BGP RECV message type 4 (KeepAlive) length 19
open	BGP open packets	Nov 28 18:37:42 bgp_send: sending 37 bytes to 10.217.5.101 (External AS 65471) Nov 28 18:37:42 Nov 28 18:37:42 BGP SEND 10.217.5.1+179 -> 10.217.5.101+38135 Nov 28 18:37:42 BGP SEND message type 1 (Open) length 37

Tracing Flags	Description	Example Output
packets	All BGP protocol packets	Sep 27 17:45:31 BGP RECV 10.0.100.108+179 -> 10.0.100.105+1033 Sep 27 17:45:31 BGP RECV message type 4 (KeepAlive) length 19 Sep 27 17:45:31 bgp_send: sending 19 bytes to 10.0.100.108 (Internal AS 100) Sep 27 17:45:31 BGP SEND 10.0.100.105+1033 -> 10.0.100.108+179 Sep 27 17:45:31 BGP SEND message type 4 (KeepAlive) length 19 Sep 27 17:45:31 bgp_read_v4_update: receiving packet(s) from 10.0.100.108 (Internal AS 100)
update	Update packets	Nov 28 19:05:24 BGP SEND 10.217.5.1+179 -> 10.217.5.101+55813 Nov 28 19:05:24 BGP SEND message type 2 (Update) length 53 Nov 28 19:05:24 bgp_send: sending 65 bytes to 10.217.5.101 (External AS 65471) Nov 28 19:05:24 Nov 28 19:05:24 BGP SEND 10.217.5.1+179 -> 10.217.5.101+55813 Nov 28 19:05:24 BGP SEND message type 2 (Update) length 65 Nov 28 19:05:24 bgp_send: sending 55 bytes to 10.217.5.101 (External AS 65471)

Step 2: Display Sent or Received BGP Packets

Action To configure the tracing for sent or received BGP protocol packets, follow these steps:

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

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

2. Configure the flag to display sent, received, or both sent and received packet information:

   ```
   [edit protocols bgp traceoptions]
   user@host# set flag update send
   ```

   or

   ```
   [edit protocols bgp traceoptions]
   user@host# set flag update receive
   ```

   or

   ```
   [edit protocols bgp traceoptions]
   user@host# set flag update
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit protocols bgp traceoptions]
   user@host# show
   file bgplog size 10k files 10;
   flag update send;
   ```

   or

   ```
   [edit protocols bgp traceoptions]
   ```

```
user@host# show
file bgplog size 10k files 10;
flag update receive;
```

or

```
[edit protocols bgp traceoptions]
user@host# show
file bgplog size 10k files 10;
flag update send receive;
```

4. Commit the configuration:

```
user@host# commit
```

5. View the contents of the file containing the detailed messages:

```
user@host# run show log filename
```

For example:

```
[edit protocols bgp traceoptions]
user@host# run show log bgplog
Sep 13 12:58:23 trace_on: Tracing to "/var/log/bgplog" started
Sep 13 12:58:23 BGP RECV flags 0x40 code ASPath(2): <null>
Sep 13 12:58:23 BGP RECV flags 0x40 code LocalPref(5): 100
Sep 13 12:58:23 BGP RECV flags 0xc0 code Extended Communities(16):
2:10458:3
[...Output truncated...]
```

Step 3: Diagnose BGP Session Establishment Problems

Action To trace BGP session establishment problems, follow these steps:

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

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

2. Configure BGP open messages:

```
[edit protocols bgp]
user@host# set traceoptions flag open detail
```

3. Verify the configuration:

```
user@host# show
```

For example:

```
[edit protocols bgp]
user@host# show
traceoptions {
    file bgplog size 10k files 10;
    flag open detail;
```

4. Commit the configuration:

   user@host# **commit**

5. View the contents of the file containing the detailed messages:

   user@host# **run show log** *filename*

   For example:

```
[edit protocols bgp]
user@host# run show log bgplog
Sep 17 17:13:14 trace_on: Tracing to "/var/log/bgplog" started
Sep 17 17:13:14 bgp_read_v4_update: done with 201.0.0.2 (Internal AS
10458) received 19 octets 0 updates 0 routes
Sep 17 17:13:15 bgp_read_v4_update: receiving packet(s) from 201.0.0.3
(Internal AS 10458)
Sep 17 17:13:15 bgp_read_v4_update: done with 201.0.0.3 (Internal AS
10458) received 19 octets 0 updates 0 routes
Sep 17 17:13:44 bgp_read_v4_update: receiving packet(s) from 201.0.0.2
(Internal AS 10458)
[...Output truncated...]
```

Configure IS-IS-Specific Options

Purpose When unexpected events or problems occur, or if you want to diagnose IS-IS adjacency establishment issues, you can view more detailed information by configuring options specific to IS-IS.

Steps To Take To configure IS-IS options, follow these steps:

1. Display Detailed IS-IS Protocol Information on page 286
2. Display Sent or Received IS-IS Protocol Packets on page 289
3. Analyze IS-IS-Link State Packets in Detail on page 291

Step 1: Display Detailed IS-IS Protocol Information

Action To trace IS-IS messages in detail, follow these steps:

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

   ```
   [edit]
   user@host# edit protocols isis traceoptions
   ```

2. Configure the flag to display detailed IS-IS protocol messages:

   ```
   [edit protocols isis traceoptions]
   user@host# set flag hello detail
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit protocols isis traceoptions]
   user@host# show
   file isislog size 10k files 10;
   flag hello detail;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

5. View the contents of the file containing the detailed messages:

   user@host# **run show log** *filename*

   For example:

```
user@host# run show log isislog
Nov 29 23:17:50 trace_on: Tracing to "/var/log/isislog" started
Nov 29 23:17:50 Sending PTP IIH on so-1/1/1.0
Nov 29 23:17:53 Sending PTP IIH on so-1/1/0.0
Nov 29 23:17:54 Received PTP IIH, source id abc-core-01 on so-1/1/0.0
Nov 29 23:17:54     from interface index 11
Nov 29 23:17:54     max area 0, circuit type l2, packet length 4469
Nov 29 23:17:54     hold time 30, circuit id 6
Nov 29 23:17:54     neighbor state up
Nov 29 23:17:54     speaks IP
Nov 29 23:17:54     area address 99.0008 (1)
Nov 29 23:17:54     IP address 10.10.10.29
Nov 29 23:17:54     4396 bytes of total padding
Nov 29 23:17:54     updating neighbor abc-core-01
Nov 29 23:17:55 Received PTP IIH, source id abc-core-02 on so-1/1/1.0
Nov 29 23:17:55     from interface index 12
Nov 29 23:17:55     max area 0, circuit type l2, packet length 4469
Nov 29 23:17:55     hold time 30, circuit id 6
Nov 29 23:17:55     neighbor state up
Nov 29 23:17:55     speaks IP
Nov 29 23:17:55     area address 99.0000 (1)
Nov 29 23:17:55     IP address 10.10.10.33
Nov 29 23:17:55     4396 bytes of total padding
Nov 29 23:17:55     updating neighbor abc-core-02
```

What It Means Table 56 lists tracing flags that can be configured specific to IS-IS and presents example output for some of the flags.

Table 56: IS-IS Protocol Tracing Flags

Tracing Flags	Description	Example Output
csn	Complete sequence number PDU (CSNP)	Nov 28 20:02:48 Sending L2 CSN on interface so-1/1/0.0 Nov 28 20:02:48 Sending L2 CSN on interface so-1/1/1.0 With the detail option. Nov 28 20:06:08 Sending L2 CSN on interface so-1/1/1.0 Nov 28 20:06:08 LSP abc-core-01.00-00 lifetime 1146 Nov 28 20:06:08 sequence 0x1c4f8 checksum 0xa1e9 Nov 28 20:06:08 LSP abc-core-02.00-00 lifetime 411 Nov 28 20:06:08 sequence 0x7435 checksum 0x5424 Nov 28 20:06:08 LSP abc-brdr-01.00-00 lifetime 465 Nov 28 20:06:08 sequence 0xf73 checksum 0xab10 Nov 28 20:06:08 LSP abc-edge-01.00-00 lifetime 1089 Nov 28 20:06:08 sequence 0x1616 checksum 0xdb29 Nov 28 20:06:08 LSP abc-edge-02.00-00 lifetime 1103 Nov 28 20:06:08 sequence 0x45cc checksum 0x6883
hello	Hello packet	Nov 28 20:13:50 Sending PTP IIH on so-1/1/1.0 Nov 28 20:13:50 Received PTP IIH, source id abc-core-01 on so-1/1/0.0 Nov 28 20:13:53 Received PTP IIH, source id abc-core-02 on so-1/1/1.0 Nov 28 20:13:57 Sending PTP IIH on so-1/1/0.0 Nov 28 20:13:58 Received PTP IIH, source id abc-core-01 on so-1/1/0.0 Nov 28 20:13:59 Sending PTP IIH on so-1/1/1.0
lsp	Link-state PDU (LSP) packets	Nov 28 20:15:46 Received L2 LSP abc-edge-01.00-00, interface so-1/1/0.0 Nov 28 20:15:46 from abc-core-01 Nov 28 20:15:46 sequence 0x1617, checksum 0xd92a, lifetime 1197 Nov 28 20:15:46 Updating L2 LSP abc-edge-01.00-00 in TED Nov 28 20:15:47 Received L2 LSP abc-edge-01.00-00, interface so-1/1/1.0 Nov 28 20:15:47 from abc-core-02 Nov 28 20:15:47 sequence 0x1617, checksum 0xd92a, lifetime 1197
lsp-generation	LSP generation packets	Nov 28 20:21:24 Regenerating L1 LSP abc-edge-03.00-00, old sequence 0x682 Nov 28 20:21:27 Rebuilding L1, fragment abc-edge-03.00-00 Nov 28 20:21:27 Rebuilt L1 fragment abc-edge-03.00-00, size 59 Nov 28 20:31:52 Regenerating L2 LSP abc-edge-03.00-00, old sequence 0x689 Nov 28 20:31:54 Rebuilding L2, fragment abc-edge-03.00-00 Nov 28 20:31:54 Rebuilt L2 fragment abc-edge-03.00-00, size 256 Nov 28 20:34:05 Regenerating L1 LSP abc-edge-03.00-00, old sequence 0x683 Nov 28 20:34:08 Rebuilding L1, fragment abc-edge-03.00-00 Nov 28 20:34:08 Rebuilt L1 fragment abc-edge-03.00-00, size 59
packets	All IS-IS protocol packets	Not available.

Tracing Flags	Description	Example Output
psn	Partial sequence number PDU (PSNP) packets	Nov 28 20:40:39 Received L2 PSN, source abc-core-01, interface so-1/1/0.0 Nov 28 20:40:39 Received L2 PSN, source abc-core-02, interface so-1/1/1.0 Nov 28 20:41:36 Sending L2 PSN on interface so-1/1/1.0 Nov 28 20:41:36 Sending L2 PSN on interface so-1/1/0.0 Nov 28 20:42:35 Received L2 PSN, source abc-core-02, interface so-1/1/1.0 Nov 28 20:42:35 LSP abc-edge-03.00-00 lifetime 1196 Nov 28 20:42:35 sequence 0x68c checksum 0x746d Nov 28 20:42:35 Received L2 PSN, source abc-core-01, interface so-1/1/0.0 Nov 28 20:42:35 LSP abc-edge-03.00-00 lifetime 1196 Nov 28 20:42:35 sequence 0x68c checksum 0x746d Nov 28 20:42:49 Sending L2 PSN on interface so-1/1/1.0 Nov 28 20:42:49 LSP abc-core-01.00-00 lifetime 1197 Nov 28 20:42:49 sequence 0x1c4fb checksum 0x9bec Nov 28 20:42:49 Sending L2 PSN on interface so-1/1/0.0 Nov 28 20:42:49 LSP abc-core-01.00-00 lifetime 1197 Nov 28 20:42:49 sequence 0x1c4fb checksum 0x9bec
spf	Shortest path first (SPF) calculations	Nov 28 20:44:01 Scheduling SPF for L1: Reconfig Nov 28 20:44:01 Scheduling multicast SPF for L1: Reconfig Nov 28 20:44:01 Scheduling SPF for L2: Reconfig Nov 28 20:44:01 Scheduling multicast SPF for L2: Reconfig Nov 28 20:44:02 Running L1 SPF Nov 28 20:44:02 L1 SPF initialization complete: 0.000099s cumulative time Nov 28 20:44:02 L1 SPF primary processing complete: 0.000303s cumulative time Nov 28 20:44:02 L1 SPF result postprocessing complete: 0.000497s cumulative time Nov 28 20:44:02 L1 SPF RIB postprocessing complete: 0.000626s cumulative time Nov 28 20:44:02 L1 SPF routing table postprocessing complete: 0.000736s cumulative time

Step 2: Display Sent or Received IS-IS Protocol Packets

Action To configure the tracing for only sent or received IS-IS protocol packets, follow these steps:

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

```
[edit]
user@host# edit protocol isis traceoptions
```

2. Configure the flag to display sent, received, or both sent and received packets:

```
[edit protocols isis traceoptions]
user@host# set flag hello send
```

or

```
[edit protocols isis traceoptions]
user@host# set flag hello receive
```

or

```
[edit protocols isis traceoptions]
user@host# set flag hello
```

3. Verify the configuration:

   user@host# **show**

   For example:

   ```
   [edit protocols isis traceoptions]
   user@host# show
   file isislog size 10k files 10;
   flag hello send;
   ```

   or

   ```
   [edit protocols isis traceoptions]
   user@host# show
   file isislog size 10k files 10;
   flag hello receive;
   ```

   or

   ```
   [edit protocols isis traceoptions]
   user@host# show
   file isislog size 10k files 10;
   flag hello send receive;
   ```

4. Commit the configuration:

   user@host# **commit**

5. View the contents of the file containing the detailed messages:

   user@host# **run show log** *filename*

   For example:

   ```
   user@host# run show log isislog
   Sep 27 18:17:01 ISIS periodic xmit to 01:80:c2:00:00:15 (IFL 2)
   Sep 27 18:17:01 ISIS periodic xmit to 01:80:c2:00:00:14 (IFL 2)
   Sep 27 18:17:03 ISIS periodic xmit to 01:80:c2:00:00:15 (IFL 2)
   Sep 27 18:17:04 ISIS periodic xmit to 01:80:c2:00:00:14 (IFL 2)
   Sep 27 18:17:06 ISIS L2 hello from 0000.0000.0008 (IFL 2) absorbed
   Sep 27 18:17:06 ISIS periodic xmit to 01:80:c2:00:00:15 (IFL 2)
   Sep 27 18:17:06 ISIS L1 hello from 0000.0000.0008 (IFL 2) absorbed
   ```

Step 3: Analyze IS-IS-Link State Packets in Detail

Action To analyze IS-IS link-state packets (LSPs) in detail, follow these steps:

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

   ```
   [edit]
   user@host# edit protocols isis traceoptions
   ```

2. Configure IS-IS open messages:

   ```
   [edit protocols isis traceoptions]
   user@host# set flag lsp detail
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit protocols isis traceoptions]
   user@host# show
   file isislog size 5m world-readable;
   flag error;
   flag lsp detail;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

5. View the contents of the file containing the detailed messages:

   ```
   user@host# run show log filename
   ```

   For example:

   ```
   user@host# run show log isislog
   Nov 28 20:17:24 Received L2 LSP abc-core-01.00-00, interface so-1/1/0.0
   Nov 28 20:17:24    from abc-core-01
   Nov 28 20:17:24    sequence 0x1c4f9, checksum 0x9fea, lifetime 1199
   Nov 28 20:17:24    max area 0, length 426
   Nov 28 20:17:24    no partition repair, no database overload
   Nov 28 20:17:24    IS type 3, metric type 0
   Nov 28 20:17:24    area address 99.0908 (1)
   Nov 28 20:17:24    speaks CLNP
   Nov 28 20:17:24    speaks IP
   Nov 28 20:17:24    dyn hostname abc-core-01
   Nov 28 20:17:24    IP address 10.10.134.11
   Nov 28 20:17:24   IP prefix: 10.10.10.0/30 metric 1 up
   Nov 28 20:17:24   IP prefix: 10.10.10.4/30 metric 5 up
   Nov 28 20:17:24   IP prefix: 10.10.10.56/30 metric 5 up
   Nov 28 20:17:24   IP prefix: 10.10.10.52/30 metric 1 up
   Nov 28 20:17:24   IP prefix: 10.10.10.64/30 metric 5 up
   Nov 28 20:17:24   IP prefix: 10.10.10.20/30 metric 5 up
   Nov 28 20:17:24   IP prefix: 10.10.10.28/30 metric 5 up
   Nov 28 20:17:24   IP prefix: 10.10.10.44/30 metric 5 up
   ```

```
Nov 28 20:17:24     IP prefix 10.10.10.0 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 1
Nov 28 20:17:24     IP prefix 10.10.10.4 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IP prefix 10.10.10.56 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IP prefix 10.10.10.52 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 1
Nov 28 20:17:24     IP prefix 10.10.10.64 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IP prefix 10.10.10.20 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IP prefix 10.10.10.28 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IP prefix 10.10.10.44 255.255.255.252
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IS neighbors:
Nov 28 20:17:24     IS neighbor abc-core-02.00
Nov 28 20:17:24     internal, metrics: default 1
[...Output truncated...]
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IS neighbor abc-brdr-01.00
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IS neighbor abc-core-02.00, metric: 1
Nov 28 20:17:24     IS neighbor abc-esr-02.00, metric: 5
Nov 28 20:17:24     IS neighbor abc-edge-03.00, metric: 5
Nov 28 20:17:24     IS neighbor abc-edge-01.00, metric: 5
Nov 28 20:17:24     IS neighbor abc-edge-02.00, metric: 5
Nov 28 20:17:24     IS neighbor abc-brdr-01.00, metric: 5
Nov 28 20:17:24    IP prefix: 10.10.134.11/32 metric 0 up
Nov 28 20:17:24    IP prefix: 10.11.0.0/16 metric 5 up
Nov 28 20:17:24    IP prefix: 10.211.0.0/16 metric 0 up
Nov 28 20:17:24     IP prefix 10.10.134.11 255.255.255.255
Nov 28 20:17:24     internal, metrics: default 0
Nov 28 20:17:24     IP prefix 10.11.0.0 255.255.0.0
Nov 28 20:17:24     internal, metrics: default 5
Nov 28 20:17:24     IP prefix 10.211.0.0 255.255.0.0
Nov 28 20:17:24     internal, metrics: default 0
Nov 28 20:17:24     Updating LSP
Nov 28 20:17:24 Updating L2 LSP abc-core-01.00-00 in TED
Nov 28 20:17:24 Analyzing subtlv's for abc-core-02.00
Nov 28 20:17:24 Analysis complete
Nov 28 20:17:24 Analyzing subtlv's for abc-esr-02.00
Nov 28 20:17:24 Analysis complete
Nov 28 20:17:24 Analyzing subtlv's for abc-edge-03.00
Nov 28 20:17:24 Analysis complete
Nov 28 20:17:24 Analyzing subtlv's for abc-edge-01.00
Nov 28 20:17:24 Analysis complete
Nov 28 20:17:24 Analyzing subtlv's for abc-edge-02.00
Nov 28 20:17:24 Analysis complete
Nov 28 20:17:24 Analyzing subtlv's for abc-brdr-01.00
Nov 28 20:17:24 Analysis complete
Nov 28 20:17:24     Scheduling L2 LSP abc-core-01.00-00 sequence 0x1c4f9
on interface so-1/1/1.0
```

Configure OSPF-Specific Options

Purpose When unexpected events or problems occur, or if you want to diagnose OSPF neighbor establishment issues, you can view more detailed information by configuring options specific to OSPF.

Steps To Take To configure OSPF options, follow these steps:

1. Diagnose OSPF Session Establishment Problems on page 293
2. Analyze OSPF Link-State Advertisement Packets in Detail on page 297

Step 1: Diagnose OSPF Session Establishment Problems

Action To trace OSPF messages in detail, follow these steps:

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

   ```
   [edit]
   user@host# edit protocols ospf traceoptions
   ```

2. Configure OSPF hello messages:

   ```
   [edit protocols ospf traceoptions]
   user@host# set flag hello detail
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit protocols ospf traceoptions]
   user@host# show
   file ospf size 5m world-readable;
   flag hello detail;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

5. View the contents of the file containing the detailed messages:

   user@host# **run show log** *filename*

   For example:

```
user@host# run show log ospf
Dec  2 16:14:24 OSPF sent Hello (1) -> 224.0.0.5 (so-1/1/3.0)
Dec  2 16:14:24   Version 2, length 44, ID 10.0.0.6, area 1.0.0.0
Dec  2 16:14:24   checksum 0xf01a, authtype 0
Dec  2 16:14:24   mask 0.0.0.0, hello_ivl 10, opts 0x2, prio 128
Dec  2 16:14:24   dead_ivl 40, DR 0.0.0.0, BDR 0.0.0.0
Dec  2 16:14:24 OSPF sent Hello (1) -> 224.0.0.5 (so-1/1/2.0)
Dec  2 16:14:24   Version 2, length 44, ID 10.0.0.6, area 1.0.0.0
Dec  2 16:14:24   checksum 0xf01a, authtype 0
Dec  2 16:14:24   mask 0.0.0.0, hello_ivl 10, opts 0x2, prio 128
Dec  2 16:14:24   dead_ivl 40, DR 0.0.0.0, BDR 0.0.0.0
Dec  2 16:14:26 OSPF rcvd Hello 10.10.10.33 -> 224.0.0.5 (so-1/1/1.0)
Dec  2 16:14:26   Version 2, length 48, ID 10.10.134.12, area 0.0.0.0
Dec  2 16:14:26   checksum 0x99b8, authtype 0
Dec  2 16:14:26   mask 255.255.255.252, hello_ivl 10, opts 0x2, prio 1
Dec  2 16:14:26   dead_ivl 40, DR 0.0.0.0, BDR 0.0.0.0
Dec  2 16:14:29 OSPF rcvd Hello 10.10.10.29 -> 224.0.0.5 (so-1/1/0.0)
Dec  2 16:14:29   Version 2, length 48, ID 10.108.134.11, area 0.0.0.0
Dec  2 16:14:29   checksum 0x99b9, authtype 0
Dec  2 16:14:29   mask 255.255.255.252, hello_ivl 10, opts 0x2, prio 1
Dec  2 16:14:29   dead_ivl 40, DR 0.0.0.0, BDR 0.0.0.0
```

What It Means Table 57 lists OSPF tracing flags and presents example output for some of the flags.

Table 57: OSPF Protocol Tracing Flags

Tracing Flags	Description	Example Output
database-description	All database description packets	Dec 2 15:44:51 RPD_OSPF_NBRDOWN: OSPF neighbor 10.10.10.29 (so-1/1/0.0) state changed from Full to Down Dec 2 15:44:51 RPD_OSPF_NBRDOWN: OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Full to Down Dec 2 15:44:55 RPD_OSPF_NBRUP: OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Init to ExStart Dec 2 15:44:55 OSPF sent DbD (2) -> 224.0.0.5 (so-1/1/1.0) Dec 2 15:44:55 Version 2, length 32, ID 10.0.0.6, area 0.0.0.0 Dec 2 15:44:55 checksum 0xf76b, authtype 0 Dec 2 15:44:55 options 0x42, i 1, m 1, ms 1, seq 0xa009eee, mtu 4470 Dec 2 15:44:55 OSPF rcvd DbD 10.10.10.33 -> 224.0.0.5 (so-1/1/1.0) Dec 2 15:44:55 Version 2, length 32, ID 10.10.134.12, area 0.0.0.0 Dec 2 15:44:55 checksum 0x312c, authtype 0 Dec 2 15:44:55 options 0x42, i 1, m 1, ms 1, seq 0x2154, mtu 4470
error	OSPF errored packets	Dec 2 15:49:34 OSPF packet ignored: no matching interface from 172.16.120.29 Dec 2 15:49:44 OSPF packet ignored: no matching interface from 172.16.120.29 Dec 2 15:49:54 OSPF packet ignored: no matching interface from 172.16.120.29 Dec 2 15:50:04 OSPF packet ignored: no matching interface from 172.16.120.29 Dec 2 15:50:14 OSPF packet ignored: no matching interface from 172.16.120.29

Tracing Flags	Description	Example Output
event	OSPF state transitions	Dec 2 15:52:35 OSPF interface ge-2/2/0.0 state changed from DR to DR Dec 2 15:52:35 OSPF interface ge-3/1/0.0 state changed from DR to DR Dec 2 15:52:35 OSPF interface ge-3/2/0.0 state changed from DR to DR Dec 2 15:52:35 OSPF interface ge-4/2/0.0 state changed from DR to DR Dec 2 15:53:21 OSPF neighbor 10.10.10.29 (so-1/1/0.0) state changed from Full to Down Dec 2 15:53:21 RPD_OSPF_NBRDOWN: OSPF neighbor 10.10.10.29 (so-1/1/0.0) state changed from Full to Down Dec 2 15:53:21 OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Full to Down Dec 2 15:53:21 RPD_OSPF_NBRDOWN: OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Full to Down Dec 2 15:53:25 OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Down to Init Dec 2 15:53:25 OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Init to ExStart Dec 2 15:53:25 RPD_OSPF_NBRUP: OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Init to ExStart Dec 2 15:53:25 OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from ExStart to Exchange Dec 2 15:53:25 OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Exchange to Full Dec 2 15:53:25 RPD_OSPF_NBRUP: OSPF neighbor 10.10.10.33 (so-1/1/1.0) state changed from Exchange to Full
flooding	Link-state flooding packets	Dec 2 15:55:21 OSPF LSA Summary 10.218.0.0 10.0.0.6 flooding on so-1/1/0.0 Dec 2 15:55:21 OSPF LSA Summary 10.218.0.0 10.0.0.6 flooding on so-1/1/1.0 Dec 2 15:55:21 OSPF LSA Summary 10.218.0.0 10.0.0.6 on no so-1/1/2.0 rexmit lists, no flood Dec 2 15:55:21 OSPF LSA Summary 10.218.0.0 10.0.0.6 on no so-1/1/3.0 rexmit lists, no flood Dec 2 15:55:21 OSPF LSA Summary 10.245.0.1 10.0.0.6 on no so-1/1/2.0 rexmit lists, no flood Dec 2 15:55:21 OSPF LSA Summary 10.245.0.1 10.0.0.6 on no so-1/1/3.0 rexmit lists, no flood
hello	Hello packets	Dec 2 15:57:25 OSPF sent Hello (1) -> 224.0.0.5 (ge-3/1/0.0) Dec 2 15:57:25 Version 2, length 44, ID 10.0.0.6, area 2.0.0.0 Dec 2 15:57:25 checksum 0xe43f, authtype 0 Dec 2 15:57:25 mask 255.255.0.0, hello_ivl 10, opts 0x2, prio 128 Dec 2 15:57:25 dead_ivl 40, DR 10.218.0.1, BDR 0.0.0.0 Dec 2 15:57:25 OSPF rcvd Hello 10.10.10.33 -> 224.0.0.5 (so-1/1/1.0) Dec 2 15:57:25 Version 2, length 48, ID 10.10.134.12, area 0.0.0.0 Dec 2 15:57:25 checksum 0x99b8, authtype 0 Dec 2 15:57:25 mask 255.255.255.252, hello_ivl 10, opts 0x2, prio 1 Dec 2 15:57:25 dead_ivl 40, DR 0.0.0.0, BDR 0.0.0.0 Dec 2 15:57:27 OSPF sent Hello (1) -> 224.0.0.5 (ge-3/2/0.0) Dec 2 15:57:27 Version 2, length 44, ID 10.0.0.6, area 2.0.0.0 Dec 2 15:57:27 checksum 0xe4a5, authtype 0 Dec 2 15:57:27 mask 255.255.0.0, hello_ivl 10, opts 0x2, prio 128 Dec 2 15:57:27 dead_ivl 40, DR 10.116.0.1, BDR 0.0.0.0 Dec 2 15:57:28 OSPF rcvd Hello 10.10.10.29 -> 224.0.0.5 (so-1/1/0.0) Dec 2 15:57:28 Version 2, length 48, ID 10.10.134.11, area 0.0.0.0 Dec 2 15:57:28 checksum 0x99b9, authtype 0 Dec 2 15:57:28 mask 255.255.255.252, hello_ivl 10, opts 0x2, prio 1 Dec 2 15:57:28 dead_ivl 40, DR 0.0.0.0, BDR 0.0.0.0

Tracing Flags	Description	Example Output
lsa-ack	Link-state acknowledgment packets	Dec 2 16:00:11 OSPF rcvd LSAck 10.10.10.29 -> 224.0.0.5 (so-1/1/0.0) Dec 2 16:00:11 Version 2, length 44, ID 10.10.134.11, area 0.0.0.0 Dec 2 16:00:11 checksum 0xcdbf, authtype 0 Dec 2 16:00:11 OSPF rcvd LSAck 10.10.10.33 -> 224.0.0.5 (so-1/1/1.0) Dec 2 16:00:11 Version 2, length 144, ID 10.10.134.12, area 0.0.0.0 Dec 2 16:00:11 checksum 0x73bc, authtype 0 Dec 2 16:00:16 OSPF rcvd LSAck 10.10.10.33 -> 224.0.0.5 (so-1/1/1.0) Dec 2 16:00:16 Version 2, length 44, ID 10.10.134.12, area 0.0.0.0 Dec 2 16:00:16 checksum 0x8180, authtype 0
lsa-request	Link-state request packets	Dec 2 16:01:38 OSPF rcvd LSReq 10.10.10.29 -> 224.0.0.5 (so-1/1/0.0) Dec 2 16:01:38 Version 2, length 108, ID 10.10.134.11, area 0.0.0.0 Dec 2 16:01:38 checksum 0xe86, authtype 0
lsa-update	Link-state update packets	Dec 2 16:09:12 OSPF built router LSA, area 0.0.0.0 Dec 2 16:09:12 OSPF built router LSA, area 1.0.0.0 Dec 2 16:09:12 OSPF built router LSA, area 2.0.0.0 Dec 2 16:09:13 OSPF sent LSUpdate (4) -> 224.0.0.5 (so-1/1/0.0) Dec 2 16:09:13 Version 2, length 268, ID 10.0.0.6, area 0.0.0.0 Dec 2 16:09:13 checksum 0x8047, authtype 0 Dec 2 16:09:13 adv count 7 Dec 2 16:09:13 OSPF sent LSUpdate (4) -> 224.0.0.5 (so-1/1/1.0) Dec 2 16:09:13 Version 2, length 268, ID 10.0.0.6, area 0.0.0.0 Dec 2 16:09:13 checksum 0x8047, authtype 0 Dec 2 16:09:13 adv count 7
packets	All OSPF packets	Not available.
packet-dump	Dump the contents of selected packet types	Not available.
spf	SPF calculations	Dec 2 16:08:03 OSPF full SPF refresh scheduled Dec 2 16:08:04 OSPF SPF start, area 1.0.0.0 Dec 2 16:08:04 OSPF add LSA Router 10.0.0.6 distance 0 to SPF list Dec 2 16:08:04 SPF elapsed time 0.000525s Dec 2 16:08:04 Stub elapsed time 0.000263s Dec 2 16:08:04 OSPF SPF start, area 2.0.0.0 Dec 2 16:08:04 OSPF add LSA Router 10.0.0.6 distance 0 to SPF list Dec 2 16:08:04 SPF elapsed time 0.000253s Dec 2 16:08:04 Stub elapsed time 0.000249s Dec 2 16:08:04 OSPF SPF start, area 0.0.0.0 Dec 2 16:08:04 OSPF add LSA Router 10.0.0.6 distance 0 to SPF list Dec 2 16:08:04 OSPF add LSA Router 10.10.134.11 distance 1 to SPF list Dec 2 16:08:04 IP nexthop so-1/1/0.0 0.0.0.0 Dec 2 16:08:04 OSPF add LSA Router 10.10.134.12 distance 1 to SPF list Dec 2 16:08:04 IP nexthop so-1/1/1.0 0.0.0.0

Step 2: Analyze OSPF Link-State Advertisement Packets in Detail

Action To analyze OSPF link-state advertisement packets in detail, follow these steps:

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

   ```
   [edit]
   user@host# edit protocols ospf traceoptions
   ```

2. Configure OSPF link-state packages:

   ```
   [edit protocols ospf traceoptions]
   user@host# set flag lsa-update detail
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit protocols ospf traceoptions]
   user@host# show
   file ospf size 5m world-readable;
   flag hello detail;
   flag lsa-update detail;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

5. View the contents of the file containing the detailed messages:

   ```
   user@host# run show log filename
   ```

   For example:

   ```
   user@host# run show log ospf
   Dec  2 16:23:47 OSPF sent LSUpdate (4) -> 224.0.0.5 (so-1/1/0.0)
   Dec  2 16:23:47   Version 2, length 196, ID 10.0.0.6, area 0.0.0.0
   Dec  2 16:23:47   checksum 0xcc46, authtype 0
   Dec  2 16:23:47   adv count 6
   Dec  2 16:23:47 OSPF sent LSUpdate (4) -> 224.0.0.5 (so-1/1/1.0)
   Dec  2 16:23:47   Version 2, length 196, ID 10.0.0.6, area 0.0.0.0
   Dec  2 16:23:47   checksum 0xcc46, authtype 0
   Dec  2 16:23:47   adv count 6
   ```