Bidirectional Forwarding Detection

This document describes how to enable the Bidirectional Forwarding Detection (BFD) protocol. BFD is a detection protocol that is designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. It includes a description of how to configure multihop BFD sessions.

BFD provides a consistent failure detection method for network administrators, in addition to fast forwarding path failure detection. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.

BFD packets carry precedence of 7, and get prioritized by default. If you are applying any policy-map to change the priority for precedence 7, then BFD packets will also get subjected for the change. Avoid BFD packets drops due to queue congestion.

**Prerequisites for Bidirectional Forwarding Detection**
- Cisco Express Forwarding and IP routing must be enabled on all participating routers

**Restrictions for Bidirectional Forwarding Detection**
- Minimum value supported on `bfd interval` command is 50ms.
- BFD templates must be used to configure 3.3ms BFD. For more information, see Creating and Configuring BFD Templates, on page 17.
• IPv6 BFD client is not supported on the ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.
• Port channel (PoCH) is not supported on the ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.
• BFD for MPLS-TP is not supported on the ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.
• BFD Echo Mode is not supported on the ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.
• Moving from echo to non-echo and non-echo to echo multiple times without any delay between each iteration may cause a few BFD sessions to flap. So multiple times echo to non-echo/non-echo to echo transition is not recommended and if this scenario is required then it should be done with a delay of at least 20 seconds at each step.
• The loopback packets are not prioritized for BFD echo sessions. Apply QoS policy to increase the priority of the packets.
• BFD packets for both, echo and non-echo sessions are not subjected to the Egress QoS. These packets are sent in the high-priority queue.

Note: The above point is applicable only on the Cisco ASR900 RSP1 and RSP2 modules.

Information About Bidirectional Forwarding Detection

BFD Operation

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes.

BFD is a detection protocol that is enabled at the interface and protocol levels. Cisco supports BFD asynchronous mode, which depends on the sending of BFD control packets between two systems to activate and maintain BFD neighbor sessions between routers. Therefore, in order for a BFD session to be created, BFD must be configured on both systems (or BFD peers). Once BFD has been enabled on the interfaces and at the router level for the appropriate protocols (NHRP and the routing protocol on overlay), a BFD session is created, BFD timers are negotiated, and the BFD peers will begin to send BFD control packets to each other at the negotiated interval.

Neighbor Relationships

BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols BGP, EIGRP, IS-IS, and OSPF. By sending rapid failure detection notices to the routing protocols in the local router to initiate the routing table recalculation process, BFD contributes to greatly reduced overall network convergence time. The figure below shows a simple network with two routers running OSPF and BFD. When OSPF discovers a neighbor (1) it sends a request to the local BFD process to initiate a BFD neighbor session with the OSPF neighbor router (2). The BFD neighbor session with the OSPF neighbor router is established (3).
The figure below shows what happens when a failure occurs in the network (1). The BFD neighbor session with the OSPF neighbor router is torn down (2). BFD notifies the local OSPF process that the BFD neighbor is no longer reachable (3). The local OSPF process tears down the OSPF neighbor relationship (4). If an alternative path is available, the routers will immediately start converging on it.

A routing protocol needs to register with BFD for every neighbor it acquires. Once a neighbor is registered, BFD initiates a session with the neighbor if a session does not already exist.

OSPF registers with BFD when:

- A neighbor finite state machine (FSM) transitions to full state.
- Both OSPF BFD and BFD are enabled.

On broadcast interfaces, OSPF establishes a BFD session only with the designated router (DR) and backup designated router (BDR), but not between any two routers in DROTHER state.

A single BFD session notifies all protocols. For example, if OSPF and PIM neighbors exist, then a single BFD session notifies both the protocols.

**BFD Detection of Failures**

Once a BFD session has been established and timer negations are complete, BFD peers send BFD control packets that act in the same manner as an IGP hello protocol to detect liveliness, except at a more accelerated rate. The following information should be noted:

- BFD is a forwarding path failure detection protocol. BFD detects a failure, but the routing protocol must take action to bypass a failed peer.
- Cisco devices will use one BFD session for multiple client protocols in the Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE, 12.0(31)S, and 12.4(4)T. For example, if a network is running
OSPF and EIGRP across the same link to the same peer, only one BFD session will be established, and BFD will share session information with both routing protocols.

**BFD Version Interoperability**

Cisco IOS Release 12.2EY and Cisco IOS Release 15.S support BFD Version 1 and BFD Version 0. All BFD sessions come up as Version 1 by default and will be interoperable with Version 0. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, if one BFD neighbor is running BFD Version 0 and the other BFD neighbor is running Version 1, the session will run BFD Version 0. The output from the `show bfd neighbors [details]` command will verify which BFD version a BFD neighbor is running.

**Note**

RSP3 supports only Version 1 and do not support BFD version interoperability.

See the Example Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default for an example of BFD version detection.

**BFD Process on the RP**

**Client Interaction**

The BFD process on the RP will handle the interaction with clients, which create and delete BFD sessions.

**Session Management for the BFD Process on the RP**

The BFD RP process will primarily own all BFD sessions on the router. It will pass the session creation and deletion requests to the BFD processes on all LCs. BFD LC sessions will have no knowledge of sessions being added or deleted by the clients. Only the BFD RP process will send session addition and deletion commands to the BFD LC process.

**Session Database Management**

The BFD RP process will maintain a database of all the BFD sessions on the router. This database will contain only the minimum required information.

**Process EXEC Commands**

The BFD RP process services the BFD `show` commands.

**BFD Support for Nonstop Forwarding with Stateful Switchover**

Typically, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Nonstop forwarding (NSF) helps to suppress routing flaps in devices that are enabled with stateful switchover (SSO), thereby reducing network instability.

NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored after a switchover. With NSF, peer networking devices do not experience routing
BFD Support for Stateful Switchover

The BFD protocol provides short-duration detection of failures in the path between adjacent forwarding engines. In network deployments that use dual RP routers or switches (to provide redundancy), the routers have a graceful restart mechanism that protects the forwarding state during a switchover between the active RP and the standby RP.

The dual RPs have variable switchover times that depend on the ability of the hardware to detect a communication failure. When BFD is running on the RP, some platforms are not able to detect a switchover before the BFD protocol times out; these platforms are referred to as slow switchover platforms.

Stateful BFD on the Standby RP

To ensure a successful switchover to the standby RP, the BFD protocol uses checkpoint messages to send session information from the active RP Cisco IOS instance to the standby RP Cisco IOS instance. The session information includes local and remote discriminators, adjacent router timer information, BFD setup information, and session-specific information such as the type of session and the session version. In addition, the BFD protocol sends session creation and deletion checkpoint messages to create or delete a session on the standby RP.

The BFD sessions on the standby RP do not receive or send packets and do not process expired timers. These sessions wait for a switchover to occur and then send packets for any active sessions so that sessions do not time out on adjacent routers.

When the BFD protocol on the standby RP is notified of a switchover it changes its state to active, registers itself with Cisco Express Forwarding so that it can receive packets, and then sends packets for any elements that have expired.

BFD also uses checkpoint messages to ensure that sessions created by clients on the active RP are maintained during a switchover. When a switchover occurs, BFD starts an SSO reclaim timer. Clients must reclaim their sessions within the duration specified by the reclaim timer or else the session is deleted.

BFD Timer Values

<table>
<thead>
<tr>
<th>Maximum Number of BFD Sessions</th>
<th>Chassis Type</th>
<th>BFD Session Type</th>
<th>Minimum Timer Value (ms)</th>
<th>Clients</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>511</td>
<td>RSP1</td>
<td>Async</td>
<td>3.3</td>
<td>BGP, OSFP, ISIS, EIGRP, MPLS-TP</td>
<td>NA</td>
</tr>
</tbody>
</table>
### BFD Support for Static Routing

Unlike dynamic routing protocols, such as OSPF and BGP, static routing has no method of peer discovery. Therefore, when BFD is configured, the reachability of the gateway is completely dependent on the state of the BFD session to the specified neighbor. Unless the BFD session is up, the gateway for the static route is considered unreachable, and therefore the affected routes will not be installed in the appropriate Routing Information Base (RIB).

For a BFD session to be successfully established, BFD must be configured on the interface on the peer and there must be a BFD client registered on the peer for the address of the BFD neighbor. When an interface is used by dynamic routing protocols, the latter requirement is usually met by configuring the routing protocol instances on each neighbor for BFD. When an interface is used exclusively for static routing, this requirement must be met by configuring static routes on the peers.

---

**Table 2: BFD Timer Values on Cisco A900-RSP2A-128, A900-RSP2A-64**

<table>
<thead>
<tr>
<th>Maximum Number of BFD Sessions</th>
<th>Chassis Type</th>
<th>BFD Session Type</th>
<th>Minimum Timer Value (ms)</th>
<th>Clients</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>255</td>
<td>RSP1</td>
<td>Echo</td>
<td>3.3</td>
<td>BGP, OSFP, ISIS, EIGRP,</td>
<td>NA</td>
</tr>
</tbody>
</table>

1 For Port-Channel, the minimum timer value is 750 multiplier 3.

**Table 3: BFD Timer Values on Cisco RSP3C-400-S**

<table>
<thead>
<tr>
<th>Maximum Number of BFD Sessions</th>
<th>Chassis Type</th>
<th>BFD Session Type</th>
<th>Minimum Timer Value (ms)</th>
<th>Clients</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1023</td>
<td>RSP2</td>
<td>Async</td>
<td>3.3</td>
<td>BGP, OSFP, ISIS, EIGRP, MPLS-TP</td>
<td>NA</td>
</tr>
<tr>
<td>1023</td>
<td>RSP2</td>
<td>Echo</td>
<td>3.3</td>
<td>BGP, OSFP, ISIS, EIGRP,</td>
<td>NA</td>
</tr>
</tbody>
</table>

2 For Port-Channel, the minimum timer value is 750 multiplier 3.

3 Port Channel is not supported on RSP3.

---

**Note**

Software sessions are supported with a timer value of 200 ms.
If a BFD configuration is removed from the remote peer while the BFD session is in the up state, the updated state of the BFD session is not signaled to IPv4 static. This will cause the static route to remain in the RIB. The only workaround is to remove the IPv4 static BFD neighbor configuration so that the static route no longer tracks BFD session state. Also, if you change the encapsulation type on a serial interface to one that is unsupported by BFD, BFD will be in a down state on that interface. The workaround is to shut down the interface, change to a supported encapsulation type, and then reconfigure BFD.

A single BFD session can be used by an IPv4 static client to track the reachability of next hops through a specific interface. You can assign a BFD group for a set of BFD-tracked static routes. Each group must have one active static BFD configuration, one or more passive BFD configurations, and the corresponding static routes to be BFD-tracked. Nongroup entries are BFD-tracked static routes for which a BFD group is not assigned. A BFD group must accommodate static BFD configurations that can be part of different VRFs. Effectively, the passive static BFD configurations need not be in the same VRF as that of the active configuration.

For each BFD group, there can be only one active static BFD session. You can configure the active BFD session by adding a static BFD configuration and a corresponding static route that uses the BFD configuration. The BFD session in a group is created only when there is an active static BFD configuration and the static route that uses the static BFD configuration. When the active static BFD configuration or the active static route is removed from a BFD group, all the passive static routes are withdrawn from the RIB. Effectively, all the passive static routes are inactive until an active static BFD configuration and a static route to be tracked by the active BFD session are configured in the group.

Similarly, for each BFD group, there can be one or more passive static BFD configurations and their corresponding static routes to be BFD-tracked. Passive static session routes take effect only when the active BFD session state is reachable. Though the active BFD session state of the group is reachable, the passive static route is added to the RIB only if the corresponding interface state is up. When a passive BFD session is removed from a group, it will not affect the active BFD session if one existed, or the BFD group reachability status.

**BFD on Multiple Hops**

Cisco IOS Release 15.1(3)S and later releases support BFD on arbitrary paths, which might span multiple network hops. The BFD Multihop feature provides subsecond forwarding failure detection for a destination more than one hop, and up to 255 hops, away.

A BFD multihop session is set up between a unique source-destination address pair provided by the client. A session can be set up between two endpoints that have IP connectivity.

You must configure the `bfd-template` and `bfd map` commands to create a multihop template and associate it with one or more maps of destinations and associated BFD timers. You can enable authentication and configure a key chain for BFD multihop sessions.

**Benefits of Using BFD for Failure Detection**

When you deploy any feature, it is important to consider all the alternatives and be aware of any trade-offs being made.

The closest alternative to BFD in conventional EIGRP, IS-IS, and OSPF deployments is the use of modified failure detection mechanisms for EIGRP, IS-IS, and OSPF routing protocols.

If you set EIGRP hello and hold timers to their absolute minimums, the failure detection rate for EIGRP falls to within a one- to two-second range.
If you use fast hellos for either IS-IS or OSPF, these Interior Gateway Protocol (IGP) protocols reduce their failure detection mechanisms to a minimum of one second.

There are several advantages to implementing BFD over reduced timer mechanisms for routing protocols:

- BFD on the CPU operates under interrupt like CEF switched traffic. EIGRP, IS-IS and OSPF protocol hellos are handled in the process switching path. This provides BFD greater scalability and reliability over protocol hellos.

- Although reducing the EIGRP, IS-IS, and OSPF timers can result in minimum detection timer of one to two seconds, BFD can provide failure detection in less than one second.

- Because BFD is not tied to any particular routing protocol, it can be used as a generic and consistent failure detection mechanism for EIGRP, IS-IS, and OSPF.

- Because some parts of BFD can be distributed to the data plane, it can be less CPU-intensive than the reduced EIGRP, IS-IS, and OSPF timers, which exist wholly at the control plane.

## How to Configure Bidirectional Forwarding Detection

### Configuring BFD Session Parameters on the Interface

The steps in this procedure show how to configure BFD on the interface by setting the baseline BFD session parameters on an interface. Repeat the steps in this procedure for each interface over which you want to run BFD sessions to BFD neighbors.

#### Summary Steps

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet number`
4. Perform one of the following steps:
   - `ip address ipv4-address mask`
   - `ipv6 address ipv6-address/mask`
5. `bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier`
6. `end`

---

**Note**

RSP3 Module eysupports only the following BFD interval timers:

3.3ms, 6.6ms, 10ms, 20ms, 50ms, 100ms, 200ms, 999ms. It is recommended that peer should also configure the same timer values.
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
  Example: Device> enable |
| Step 2 configure terminal | Enters global configuration mode.  
  Example: Device# configure terminal |
| Step 3 interface gigabitethernet number | Specifies the Gigabit Ethernet interface and enters interface configuration mode.  
  Example: Device(config)# interface gigabitethernet 0/0/0 |
| Step 4 Perform one of the following steps:  
  • ip address ipv4-address mask  
  • ipv6 address ipv6-address/mask | Configures an IP address for the interface.  
  Example: Configuring an IPv4 address for the interface:  
  Device(config-if)# ip address 10.201.201.1 255.255.255.0  
  Configuring an IPv6 address for the interface:  
  Device(config-if)# ipv6 address 2001:db8:1:1::1/32 |
| Step 5 bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier | Enables BFD on the interface.  
  The bfd interval configuration is removed when the subinterface on which it is configured is removed.  
  The bfd interval configuration is not removed when:  
  • an IPv4 address is removed from an interface  
  • an IPv6 address is removed from an interface  
  • IPv6 is disabled from an interface  
  • an interface is shutdown  
  • IPv4 CEF is disabled globally or locally on an interface  
  • IPv6 CEF is disabled globally or locally on an interface  
  Example: Device(config-if)# bfd interval 50 min_rx 50 multiplier 5 |
### Configuring BFD Support for Static Routing

Perform this task to configure BFD support for static routing. Repeat the steps in this procedure on each BFD neighbor. For more information, see the "Example: Configuring BFD Support for Static Routing" section.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. Perform one of the following steps:
   - ip address ipv4-address mask
   - ipv6 address ipv6-address/mask
5. bfd interval milliseconds mix_rx milliseconds multiplier interval-multiplier
6. exit
7. ip route static bfd interface-type interface-number ip-address [group group-name [passive]]
8. ip route [vrf vrf-name] prefix mask {ip-address | interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]
9. exit
10. show ip static route
11. show ip static route bfd
12. exit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface serial 2/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Perform one of the following steps:</td>
<td>Configures an IP address for the interface.</td>
</tr>
<tr>
<td>• ip address ipv4-address mask</td>
<td></td>
</tr>
<tr>
<td>• ipv6 address ipv6-address/mask</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Configuring an IPv4 address for the interface: Device(config-if)# ip address 10.201.201.1 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Configuring an IPv6 address for the interface: Device(config-if)# ipv6 address 2001:db8:1:1::1/32</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> bfd interval milliseconds mix_rx milliseconds multiplier interval-multiplier</td>
<td>Enables BFD on the interface. The bfd interval configuration is removed when the subinterface on which it is configured is removed. The bfd interval configuration is not removed when:</td>
</tr>
<tr>
<td></td>
<td>• an IPv4 address is removed from an interface</td>
</tr>
<tr>
<td></td>
<td>• an IPv6 address is removed from an interface</td>
</tr>
<tr>
<td></td>
<td>• IPv6 is disabled from an interface</td>
</tr>
<tr>
<td></td>
<td>• an interface is shutdown</td>
</tr>
<tr>
<td></td>
<td>• IPv4 CEF is disabled globally or locally on an interface</td>
</tr>
<tr>
<td></td>
<td>• IPv6 CEF is disabled globally or locally on an interface</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# bfd interval 500 min_rx 500 multiplier 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring BFD Echo Mode

BFD echo mode is enabled by default, but you can disable it such that it can run independently in each direction.

BFD echo mode works with asynchronous BFD. Echo packets are sent by the forwarding engine and forwarded back along the same path in order to perform detection—the BFD session at the other end does not participate in the actual forwarding of the echo packets. The echo function and the forwarding engine are responsible for

### Command or Action

<table>
<thead>
<tr>
<th>Step 7</th>
<th>ip route static bfd interface-type interface-number ip-address [group group-name [passive]]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# ip route static bfd serial 2/0 10.1.1.1 group group1 passive</td>
</tr>
</tbody>
</table>

**Purpose**: Specifies a static route BFD neighbor.  
- The `interface-type`, `interface-number`, and `ip-address` arguments are required because BFD support exists only for directly connected neighbors.

| Step 8 | ip route [vrf vrf-name] prefix mask {ip-address | interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag] |
|------|---------------------------------------------------------------|
| Example: | Device(config)# ip route 10.0.0.0 255.0.0.0 |

**Purpose**: Specifies a static route BFD neighbor.

<table>
<thead>
<tr>
<th>Step 9</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# exit</td>
</tr>
</tbody>
</table>

**Purpose**: Exits global configuration mode and returns to privileged EXEC mode.

<table>
<thead>
<tr>
<th>Step 10</th>
<th>show ip static route</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# show ip static route</td>
</tr>
</tbody>
</table>

(Optional) Displays static route database information.

<table>
<thead>
<tr>
<th>Step 11</th>
<th>show ip static route bfd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# show ip static route bfd</td>
</tr>
</tbody>
</table>

(Optional) Displays information about the static BFD configuration from the configured BFD groups and nongroup entries.

<table>
<thead>
<tr>
<th>Step 12</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# exit</td>
</tr>
</tbody>
</table>

Exits privileged EXEC mode and returns to user EXEC mode.

---

### Configuring BFD Echo Mode

BFD echo mode is enabled by default, but you can disable it such that it can run independently in each direction. BFD echo mode works with asynchronous BFD. Echo packets are sent by the forwarding engine and forwarded back along the same path in order to perform detection—the BFD session at the other end does not participate in the actual forwarding of the echo packets. The echo function and the forwarding engine are responsible for
the detection process; therefore, the number of BFD control packets that are sent out between two BFD neighbors is reduced. In addition, because the forwarding engine is testing the forwarding path on the remote (neighbor) system without involving the remote system, there is an opportunity to improve the interpacket delay variance, thereby achieving quicker failure detection times than when using BFD Version 0 with BFD control packets for the BFD session.

Echo mode is described as without asymmetry when it is running on both sides (both BFD neighbors are running echo mode).

**BFD Slow Timer**

BFD can use the slow timer to slow down the asynchronous session when the echo mode is enabled, and reduce the number of BFD control packets that are sent between two BFD neighbors. Also, the forwarding engine tests the forwarding path on the remote (neighbor) system without involving the remote system, so there is less interpacket delay variability and faster failure detection times.

**Prerequisites**

BFD must be running on all participating routers.

Before using BFD echo mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the `no ip redirects` command, in order to avoid high CPU utilization.

The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured. See the Configuring BFD Session Parameters on the Interface section for more information.

**Restrictions**

The following restriction apply when configuring BFD:

BFD Echo Mode is not supported on the ASR 900 RSP3 Module.

In case, if you bring up an echo BFD session, following error message is displayed:

**BFD template model:**

Please remove bfd template <template name> from the interface
add no echo to template
reapply bfd template <template name> on interface

**BFD legacy configuration:**

removal bfd interval <value> min_rx <value> multiplier <value> or no bfd interval will also suffice
Now remove the bfd client configurations also i.e Ex the client is ospf remove bfd all-interfaces under ospf
Apply the bfd interval <value> min_rx <value>
multiplier <value>
add no bfd echo
add back the bfd client configuration

In Case, if you configure BFD in non-echo mode and then move to echo RSP3, following error message is displayed:

"Echo Mode for ld = 0x%x not supported on RSP3\n"
"add no echo to template name if configured via template\n"
"or add no bfd echo to interface if configured\n"
"via legacy(i.e bfd interval on the interface)"
Configuring the BFD Slow Timer

The steps in this procedure show how to change the value of the BFD slow timer. Repeat the steps in this procedure for each BFD router.

SUMMARY STEPS

1. enable
2. configure terminal
3. bfd slow-timer milliseconds
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>bfd slow-timer milliseconds</td>
<td>Configures the BFD slow timer.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# bfd slow-timer 12000</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits global configuration mode and returns the router to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Disabling BFD Echo Mode Without Asymmetry

The steps in this procedure show how to disable BFD echo mode without asymmetry—no echo packets will be sent by the router, and the router will not forward BFD echo packets that are received from any neighbor routers.

Repeat the steps in this procedure for each BFD router.
SUMMARY STEPS

1. enable
2. configure terminal
3. no bfd echo
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 no bfd echo</td>
<td>Disables BFD echo mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Use the no form to disable BFD echo mode.</td>
</tr>
<tr>
<td>Router(config)# no bfd echo</td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Creating and Configuring BFD Templates

Perform this task to create a BFD template, enter BFD configuration mode, and configure BFD interval timers.

**Note**
ASR 900 RSP3 Module for Cisco IOS XE Release 3.16 supports only the following BFD interval timers: 3.3ms, 6.6ms, 10ms, 20ms, 50ms, 100ms, 200ms, 999ms.
### SUMMARY STEPS

1. enable
2. configure terminal
3. bfd-template single-hop  template-name
4. interval min-tx  milliseconds  min-rx  milliseconds  multiplier  multiplier-value
5. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: | Device> enable |
| **Step 2** | configure terminal | Enters global configuration mode. |
| Example: | Device# configure terminal |
| **Step 3** | bfd-template single-hop  template-name | Creates a BFD template and enters BFD configuration mode. |
| Example: | Device(config)# bfd-template single-hop bfdtemplate1 |
| **Step 4** | interval min-tx  milliseconds  min-rx  milliseconds  multiplier  multiplier-value | Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable. |
| Example: | Device(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3 |
| **Step 5** | end | Exits BFD configuration mode and returns the device to privileged EXEC mode. |
| Example: | Device(bfd-config)# end |
Creating and Configuring BFD Templates

You can configure a single-hop template to specify a set of BFD interval values. BFD interval values specified as part of the BFD template are not specific to a single interface. You can configure a multihop template to associate these values with one or more maps of destinations and associated BFD timers. You can enable authentication and configure a key chain for BFD multihop sessions.

Configuring a Single-Hop Template

Perform this task to create a BFD single-hop template and configure BFD interval timers.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `bfd-template single-hop template-name`
4. `interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value`
5. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: | Router> enable |
| Step 2 | `configure terminal` | Enters global configuration mode. |
| Example: | Router# configure terminal |
| Step 3 | `bfd-template single-hop template-name` | Creates a single-hop BFD template and enters BFD configuration mode. |
| Example: | Router(config)# bfd-template single-hop bfdtemplate1 |
| Step 4 | `interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value` | Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable. |
| Example: | Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3 |
### Configuring a Multihop Template

Perform this task to create a BFD multihop template and configure BFD interval timers, authentication, and key chain.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **bfd-template multi-hop template-name**
4. **interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value**
5. **authentication authentication-type keychain keychain-name**
6. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a BFD multihop BFD template and enters BFD configuration mode.</td>
</tr>
<tr>
<td><strong>bfd-template multi-hop template-name</strong></td>
<td>Creates a BFD multihop BFD template and enters BFD configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# bfd-template multi-hop mh-template1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD</td>
</tr>
</tbody>
</table>
### Configuring a BFD Map

Perform this task to configure a BFD map that associates the interval timers and authentication configured in a template with unique source-destination address pairs for multihop BFD sessions.

#### Before You Begin

You must configure a BFD multihop template before you associate it with a map.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bfd map ipv4 vrf vrf-name destination length source-address length template-name**
4. **end**

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> authentication authentication-type keychain keychain-name</td>
<td>Configures authentication for the multihop template and specifies the authentication type.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(bfd-config)# authentication key-md5 keychain bfd-multihop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits BFD configuration mode and returns the router to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(bfd-config)# end</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td>3</td>
<td><code>bfd map ipv4 vrf vrf-name destination length source-address length template-name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# bfd map ipv4 vrf vpn1 192.168.0.0/24 192.168.42.5/32 mh-template1</code></td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# end</code></td>
</tr>
</tbody>
</table>

## Configuration Examples for Bidirectional Forwarding Detection

### Example: Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default

In the following example, the EIGRP network contains RouterA, RouterB, and RouterC. The Gigabit Ethernet interface 0/0/1 on RouterA is connected to the same network as Gigabit Ethernet interface 0/0/1 on RouterB. The Gigabit Ethernet interface 0/0/1 on RouterB is connected to the same network as Gigabit Ethernet interface 0/0/1 on RouterC.

RouterA and RouterB are running BFD Version 1, which supports echo mode, and RouterC is running BFD Version 0, which does not support echo mode. The BFD sessions between RouterC and its BFD neighbors are said to be running echo mode with asymmetry because echo mode will run on the forwarding path for RouteA and RouterB, and their echo packets will return along the same path for BFD sessions and failure detections, while their BFD neighbor RouterC runs BFD Version 0 and uses BFD controls packets for BFD sessions and failure detections.

The example, starting in global configuration mode, shows the configuration of BFD.

### Configuration for RouterA

```
interface GigabtetherenN0/0/0
no shutdown
ip address 10.4.9.14 255.255.255.0
duplex auto
speed auto
```
! interface Gigabtethernet0/0/1
    ip address 172.16.1.1 255.255.255.0
    bfd interval 50 min_rx 50 multiplier 3
    no shutdown
duplex auto
    speed auto
!
router eigrp 11
    network 172.16.0.0
    bfd all-interfaces
    auto-summary
!
    ip default-gateway 10.4.9.1
    ip default-network 0.0.0.0
    ip route 0.0.0.0 0.0.0.0 10.4.9.1
    ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
exec-timeout 30
    stopbits 1
line aux 0
    stopbits 1
line vty 0 4
login
!
end

Configuration for RouterB

!
interface Gigabtethernet0/0/0
    no shutdown
    ip address 10.4.9.34 255.255.255.0
duplex auto
    speed auto
!
interface Gigabtethernet0/0/1
    ip address 172.16.1.2 255.255.255.0
    bfd interval 50 min_rx 50 multiplier 3
    no shutdown
duplex auto
    speed auto
!
router eigrp 11
    network 172.16.0.0
    bfd all-interfaces
    auto-summary
!
ip default-gateway 10.4.9.1
    ip default-network 0.0.0.0
    ip route 0.0.0.0 0.0.0.0 10.4.9.1
    ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
in ip http server
!
logging alarm informational
!
control-plane
!
line con 0
exec-timeout 30
    stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!

Configuration for RouterC

!
interface Gigabtethernet0/0/0
  no shutdown
  ip address 10.4.9.34 255.255.255.0
duplex auto
  speed auto
interface Gigabtethernet0/0/1
  ip address 172.16.1.2 255.255.255.0
  bfd interval 50 min_rx 50 multiplier 3
  no shutdown
duplex auto
  speed auto
router eigrp 11
  network 172.16.0.0
  bfd all-interfaces
  auto-summary
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
no ip http server
logging alarm informational
control-plane
!
line con 0
  exec-timeout 30 0
stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  login
  
!
end

The output from the show bfd neighbors details command from RouterA verifies that BFD sessions have been created among all three routers and that EIGRP is registered for BFD support. The first group of output shows that RouterC with the IP address 172.16.1.3 runs BFD Version 0 and therefore does not use the echo mode. The second group of output shows that RouterB with the IP address 172.16.1.2 does run BFD Version 1, and the 50 millisecond BFD interval parameter had been adopted. The relevant command output is shown in bold in the output.

RouterA# show bfd neighbors details

<table>
<thead>
<tr>
<th>OurAddr</th>
<th>NeighAddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>LD/RD</td>
<td>RH/RS</td>
</tr>
<tr>
<td>172.16.1.1</td>
<td>172.16.1.3</td>
</tr>
</tbody>
</table>

Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
The output from the `show bfd neighbors details` command on Router B verifies that BFD sessions have been created and that EIGRP is registered for BFD support. As previously noted, RouterA runs BFD Version 1, therefore echo mode is running, and RouterC runs BFD Version 0, so echo mode does not run. The relevant command output is shown in bold in the output.
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(5735)
Rx Count: 5731, Rx Interval (ms) min/max/avg: 32/72/49 last: 32 ms ago
Tx Count: 5740, Tx Interval (ms) min/max/avg: 40/64/50 last: 44 ms ago
Registered protocols: EIGRP
Uptime: 00:04:45

Last packet: Version: 0
- Diagnostic: 0
  I Hear You bit: 1 - Demand bit: 0
  Poll bit: 0 - Final bit: 0
  Multiplier: 3 - Length: 24
  My Discr.: 6 - Your Discr.: 3
  Min tx interval: 50000 - Min rx interval: 50000
  Min Echo interval: 0

When Gigabit ethernet interface 0/0/1 on RouterB fails, BFD will no longer detect Router B as a BFD neighbor for RouterA or for RouterC. In this example, Gigabit Ethernet interface 0/0/1 has been administratively shut down on RouterB.

The following output from the `show bfd neighbors` command on RouterA now shows only one BFD neighbor for RouterA in the EIGRP network. The relevant command output is shown in bold in the output.

```
RouterA# show bfd neighbors
OurAddr NeighAddr
LD/RD RH/RS Holdown(mult) State Int
172.16.1.1 172.16.1.3
   5/3 1(RH) 134 (3 ) Up Gig0/0/1
```

The following output from the `show bfd neighbors` command on RouterC also now shows only one BFD neighbor for RouterC in the EIGRP network. The relevant command output is shown in bold in the output.

```
RouterC# show bfd neighbors
OurAddr NeighAddr
LD/RD RH Holdown(mult) State Int
172.16.1.3 172.16.1.1
   3/5 1 114 (3 ) Up Gig0/0/1
```

### Example: Configuring BFD in an OSPF Network

In the following example, the simple OSPF network consists of Router A and Router B. Gigabit Ethernet interface 0/0/1 on Router A is connected to the same network as Gigabit Ethernet interface 0/0/1 in Router B. The example, starting in global configuration mode, shows the configuration of BFD. For both Routers A and B, BFD is configured globally for all interfaces associated with the OSPF process.

```
Configuration for Router A

! interface Gigabitethernet 0/0/1
  ip address 172.16.10.1 255.255.255.0
  bfd interval 50 min_rx 50 multiplier 3
! interface Gigabitethernet 0/0/0
  ip address 172.17.0.1 255.255.255.0

router ospf
```

IP Routing: BFD Configuration Guide, Cisco IOS XE Everest 16.5.1 (Cisco ASR 900 Series)
Configuration for Router B

```
! interface Gigabitethernet 0/0/1
  ip address 172.16.10.2 255.255.255.0
  bfd interval 50 min_rx 50 multiplier 3
! interface Gigabitethernet 0/0/0
! router ospf 123
  log-adjacency-changes detail
  network 172.16.0.0 0.0.255.255 area 0
  network 172.18.0.0 0.0.255.255 area 0
  bfd all-interfaces
```

The output from the `show bfd neighbors details` command verifies that a BFD session has been created and that OSPF is registered for BFD support. The relevant command output is shown in bold in the output.

Router A

```
RouterA# show bfd neighbors details
OurAddr NeighAddr LD/RD RH Holdown(mult) State Int
172.16.10.1 172.16.10.2 1/2 1 532 (3 ) Up Gig0/0/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 0
I Hear You bit: 1 - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 3 - Length: 24
My Discr.: 2 - Your Discr.: 1
Min tx interval: 50000 - Min rx interval: 1000
Min Echo interval: 0
```

The output from the `show bfd neighbors details` command from Router B verifies that a BFD session has been created:

Router B

```
Router> show bfd neighbors details
OurAddr NeighAddr LD/RD RH Holdown(mult) State Int
172.16.10.2 172.16.10.1 8/1 1 1000 (5 ) Up Gig0/0/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0
I Hear You bit: 1 - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 5 - Length: 24
My Discr.: 1 - Your Discr.: 8
Min tx interval: 200000 - Min rx interval: 200000
```
Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
IPC Tx Failure Count: 0
IPC Rx Failure Count: 0
Total Adjts Found: 1

The output of the `show ip ospf` command verifies that BFD has been enabled for OSPF. The relevant command output is shown in bold in the output.

**Router A**

```
RouterA# show ip ospf
Routing Process "ospf 123" with ID 172.16.10.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
BFD is enabled

Area BACKBONE(0)
  Number of interfaces in this area is 2 (1 loopback)
  Area has no authentication
  SPF algorithm last executed 00:00:08.828 ago
  SPF algorithm executed 9 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x028417
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

**Router B**

```
RouterB# show ip ospf
Routing Process "ospf 123" with ID 172.18.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x0
```
Number of opaque AS LSA 0.Checksum Sum 0x0
Number of Dcbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
BFD is enabled

Area BACKBONE(0)
  Number of interfaces in this area is 2 (1 loopback)
  Area has no authentication
  SPF algorithm last executed 02:07:30.932 ago
  SPF algorithm executed 7 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x28417
  Number of opaque link LSA 0. Checksum Sum 0x0
  Number of Dcbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0

The output of the show ip ospf interface command verifies that BFD has been enabled for OSPF on the interfaces connecting Router A and Router B. The relevant command output is shown in bold in the output.

**Router A**

RouterA# show ip ospf interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
Internet Address 172.16.10.1/24, Area 0
Process ID 123, Router ID 172.16.10.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1, **BFD enabled**
Designated Router (ID) 172.18.0.1, Interface address 172.16.10.2
Backup Designated router (ID) 172.16.10.1, Interface address 172.16.10.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.18.0.1 (Designated Router)
  Suppress hello for 0 neighbor(s)

**Router B**

RouterB# show ip ospf interface Gigabit Ethernet 0/0/0
GigabitEthernet0/0/1 is up, line protocol is up
Internet Address 172.18.0.1/24, Area 0
Process ID 123, Router ID 172.18.0.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1, **BFD enabled**
Designated Router (ID) 172.18.0.1, Interface address 172.18.0.1
Backup Designated router (ID) 172.18.0.1, Interface address 172.18.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Example: Configuring BFD in a BGP Network

In the following example, the simple BGP network consists of Router A and Router B. The Gigabit Ethernet interface 0/0/1 on Router A is connected to the same network as Gigabit Ethernet interface 0/0/1 in Router B. The example, starting in global configuration mode, shows the configuration of BFD.

Configuration for Router A

```
interface GigabitEthernet 0/0/1
  ip address 172.16.10.1 255.255.255.0
  bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet 0/0/0
  ip address 172.17.0.1 255.255.255.0
!
router bgp 40000
  bgp log-neighbor-changes
  neighbor 172.16.10.2 remote-as 45000
  neighbor 172.16.10.2 fall-over bfd
!
  address-family ipv4
    neighbor 172.16.10.2 activate
    no auto-summary
    no synchronization
    network 172.18.0.0 mask 255.255.255.0
    exit-address-family
!
```

Configuration for Router B

```
interface GigabitEthernet 0/0/1
  ip address 172.16.10.2 255.255.255.0
  bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet 0/0/0
  ip address 172.18.0.1 255.255.255.0
!
router bgp 45000
  bgp log-neighbor-changes
  neighbor 172.16.10.1 remote-as 40000
  neighbor 172.16.10.1 fall-over bfd
!
  address-family ipv4
    neighbor 172.16.10.1 activate
    no auto-summary
    no synchronization
    network 172.17.0.0 mask 255.255.255.0
    exit-address-family
!
```

The output from the `show bfd neighbors details` command from Router A verifies that a BFD session has been created and that BGP is registered for BFD support. The relevant command output is shown in bold in the output.

Router A

```
RouterA# show bfd neighbors details

OurAddr    NeighAddr     LD/RD RH Holdown(mult) State    Int
172.16.10.1 172.16.10.2  1/8 1 332 (3 ) Up    Gig0/0/1
```
The output from the `show bfd neighbors details` command on Router B verifies that a BFD session has been created:

**Router B**

RouterB# show bfd neighbors details

Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
IPC Tx Failure Count: 0
IPC Rx Failure Count: 0
Total Adjts Found: 1

The output of the `show ip bgp neighbors` command verifies that BFD has been enabled for the BGP neighbors:

**Router A**

RouterA# show ip bgp neighbors

BGP neighbor is 172.16.10.2, remote AS 45000, external link
  Using BFD to detect fast failover

**Router B**

RouterB# show ip bgp neighbors

BGP neighbor is 172.16.10.1, remote AS 40000, external link
  Using BFD to detect fast failover
Example: Configuring BFD in an IS-IS Network

In the following example, the simple IS-IS network consists of Router A and Router B. The Gigabit Ethernet interface 0/0/1 on Router A is connected to the same network as Gigabit Ethernet interface 0/0/0 for Router B. The example, starting in global configuration mode, shows the configuration of BFD.

Configuration for Router A

```
! interface GigabitEthernet 0/0/1
 ip address 172.16.10.1 255.255.255.0
 ip router isis
 bfd interval 50 min_rx 50 multiplier 3
 ! interface GigabitEthernet 0/0/0
 ip address 172.17.0.1 255.255.255.0
 ip router isis
 !
 router isis
 net 49.0001.1720.1600.1001.00
 bfd all-interfaces
```

Configuration for Router B

```
! interface GigabitEthernet 0/0/0
 ip address 172.16.10.2 255.255.255.0
 ip router isis
 bfd interval 50 min_rx 50 multiplier 3
 ! interface GigabitEthernet 0/0/1
 ip address 172.18.0.1 255.255.255.0
 ip router isis
 !
 router isis
 net 49.0000.0000.0002.00
 bfd all-interfaces
```

The output from the `show bfd neighbors details` command from Router A verifies that a BFD session has been created and that IS-IS is registered for BFD support:

```
RouterA# show bfd neighbors details

OurAddr  NeighAddr  LD/RO RH  Holdown(mult) State  Int
172.16.10.1  172.16.10.2  1/8  1  536 (3 )  Up  Gig0/0/1

Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 1000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(3543)
Tx Count: 13877, Rx Interval (ms) min/max/avg: 200/448/335 last: 64 ms ago
Tx Count: 23546, Tx Interval (ms) min/max/avg: 152/248/196 last: 32 ms ago
Registered protocols: ISIS
Uptime: 01:17:09
Last packet: Version: 0 - Diagnostic: 0
 I Hear You bit: 1 - Demand bit: 0
 Poll bit: 0 - Final bit: 0
 Multiplier: 3 - Length: 24
 My Discr.: 8 - Your Discr.: 1
 Min tx interval: 50000 - Min rx interval: 1000
 Min Echo interval: 0
```
The output from the `show bfd neighbors details` command from the line card on Router B verifies that a BFD session has been created:

```
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr    LD/RD RH Holdown(mult) State Int
172.16.10.2    172.16.10.1   8/1 1 1000 (5 ) Up    Gig0/0/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0 - Diagnostic: 0
              I Hear You bit: 1 - Demand bit: 0
              Poll bit: 0 - Final bit: 0
Multiplier: 5 - Length: 24
My Discr.: 1 - Your Discr.: 8
Min tx interval: 200000 - Min rx interval: 200000
Up time: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
IPC Tx Failure Count: 0
IPC Rx Failure Count: 0
Total Adjs Found: 1
```

**Example: Configuring BFD in an HSRP Network**

In the following example, the HSRP network consists of Router A and Router B. The Gigabit Ethernet interface 2/0 on Router A is connected to the same network as Gigabit Ethernet interface 2/0 on Router B. The example, starting in global configuration mode, shows the configuration of BFD.

```
Router A

ip cef
interface GigabitEthernet0/0/1
no shutdown
ip address 10.0.0.2 255.0.0.0
ip router-cache cef
bfd interval 200 min_rx 200 multiplier 3
standby 1 ip 10.0.0.11
standby 1 preempt
standby 1 priority 110
standby 2 ip 10.0.0.12
standby 2 preempt
standby 2 priority 110
```

Note

In the following example, the `standby bfd` and the `standby bfd all-interfaces` commands are not displayed. HSRP support for BFD peering is enabled by default when BFD is configured on the router or interface using the `bfd interval` command. The `standby bfd` and `standby bfd all-interfaces` commands are needed only if BFD has been manually disabled on a router or interface.
Example: Configuring BFD Support for Static Routing

In the following example, the network consists of Device A and Device B. Serial interface 2/0 on Device A is connected to the same network as serial interface 2/0 on Device B. In order for the BFD session to come up, Device B must be configured.

Device A

configure terminal
interface Serial 2/0
ip address 10.201.201.1 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.2
ip route 10.0.0.0 255.0.0.0 Serial 2/0 10.201.201.2

Device B

configure terminal
interface Serial 2/0
ip address 10.201.201.2 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.1
ip route 10.0.0.0 255.0.0.0 Serial 2/0 10.201.201.1

Note that the static route on Device B exists solely to enable the BFD session between 10.201.201.1 and 10.201.201.2. If there is no useful static route that needs to be configured, select a prefix that will not affect packet forwarding, for example, the address of a locally configured loopback interface.

In the following example, there is an active static BFD configuration to reach 209.165.200.225 through Gigabit Ethernet interface 0/0/0 in the BFD group testgroup. As soon as the static route is configured that is tracked
by the configured static BFD, a single hop BFD session is initiated to 209.165.200.225 through Ethernet interface 0/0. The prefix 10.0.0.0/8 is added to the RIB if a BFD session is successfully established.

```
configure terminal
ip route static bfd GigabitEthernet 0/0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
```

In the following example, a BFD session to 209.165.200.226 through Ethernet interface 0/0.1001 is marked to use the group testgroup. That is, this configuration is a passive static BFD. Though there are static routes to be tracked by the second static BFD configuration, a BFD session is not triggered for 209.165.200.226 through Gigabit Ethernet interface 0/0/0. The existence of the prefixes 10.1.1.1/8 and 10.2.2.2/8 is controlled by the active static BFD session (Gigabit Ethernet interface 0/0/0 209.165.200.225).

```
configure terminal
ip route static bfd GigabitEthernet 0/0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
ip route static bfd Ethernet 0/0.1001 209.165.200.226 group testgroup passive
ip route 10.1.1.1 255.255.255.224 GigabitEthernet 0/0/0 209.165.200.226
ip route 10.2.2.2 255.255.255.224 GigabitEthernet 0/0/0 209.165.200.226
```
Example: Configuring BFD Support for Static Routing