IP Routing: BFD Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
IS-IS BFD Topology 45
IS-IS BFD IPv6 Session Creation 46
IS-IS BFD IPv6 Session Deletion 46
How to Configure ISIS IPv6 Client for BFD 46
  Configuring IS-IS IPv6 Client Support for BFD on an Interface 46
  Configuring IS-IS IPv6 Client Support for BFD on All Interfaces 47
Configuration Examples for ISIS IPv6 Client for BFD 48
  Example: IS-IS IPv6 Client Support for BFD on a Single Interface 48
  Example: IS-IS IPv6 Client Support for BFD on All Interfaces 49

CHAPTER 5  BFD IPv6 Encapsulation Support 51
Prerequisites for BFD IPv6 Encapsulation Support 51
Restrictions for BFD IPv6 Encapsulation Support 51
Information About BFD IPv6 Encapsulation Support 51
  Overview of the BFDv6 Protocol 51
  BFDv6 Registration 52
  BFDv6 Global and Link-Local Addresses 52
  BFD for IPv4 and IPv6 on the Same Interface 52
How to Configure BFD IPv6 Encapsulation Support 53
  Configuring BFD Session Parameters on the Interface 53
Configuration Examples for BFD IPv6 Encapsulation Support 54
  Example: Configuring BFD Session Parameters on the Interface 54

CHAPTER 6  Configuring BFD Debug Enhancement 57
Finding Feature Information 57
Prerequisites for BFD Debug Enhancement 57
Restrictions for BFD Debug Enhancement 57
Information About BFD Debug Enhancement 58
  Overview of BFD Debug Enhancement 58
    BFD Debug Enhancement - Event Tracer subsystem 58
    BFD Debug Enhancement - Event Log Architecture 58
How to Configure BFD Debug Enhancement 58
  Configuring BFD Debug Enhancement 58
Configuration Examples for BFD Debug Enhancement 60
## Example: Configuring BFD Debug Enhancement 60
## Additional References for BFD Debug Enhancement 61
## Feature Information for BFD Debug Enhancement 62

---

### CHAPTER 7

**Bidirectional Forwarding Detection Configuration of Deterministic Hardware Offload** 65

- Information About BFD Deterministic Hardware Offload 66
- Configuring BFD Deterministic Hardware Offload 66
- Example for Configuring BFD Deterministic Hardware Offload 67
- Related Documents 67
- Standards 67
CHAPTER 1

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.

Note

BFD packets carries 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, on page 1
- Restrictions for Bidirectional Forwarding Detection, on page 1
- Information About Bidirectional Forwarding Detection, on page 2
- How to Configure Bidirectional Forwarding Detection, on page 8
- Configuration Examples for Bidirectional Forwarding Detection, on page 19

Prerequisites for Bidirectional Forwarding Detection

- Cisco Express Forwarding and IP routing must be enabled on all participating routers

Restrictions for Bidirectional Forwarding Detection

- BFD dampening feature is not supported on the Cisco ASR 900 Series Routers.
- 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 16.
For BFD over IPv6 hardware offload and software based sessions, only async mode is supported on the RSP3 module. Echo mode is not supported.

Starting with Cisco IOS XE Release 3.18SP, BFD over PoCH is supported on the RSP3 module in software offload mode only. The minimum timer value supported is 200 milliseconds.

BFD for MPLS-TP is not supported on the RSP3 module in Cisco IOS XE Release 3.16.

BFD Echo Mode is not supported on the RSP3 module in Cisco IOS XE Release 3.16.

Starting with Cisco IOS XE Fuji Release 16.9.1, BFD Echo mode is supported in the RSP3 module.

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. This is applicable only on the Cisco ASR900 RSP1 and RSP2 modules.

BFD with authentication is supported only in software. Hardware offload is not supported for BFD with authentication.

The minimum timer value supported for the BFD software session is 200 ms.

BFD over IPv4 unicast GRE tunnel is not supported.

---

**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.

Note: 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 15.5 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 flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and forwarding processors to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.
In devices that support dual RPs, SSO establishes one of the RPs as the active processor; the other RP is designated as the standby processor, and then synchronizes information between them. A switchover from the active to the standby processor occurs when the active RP fails, when it is removed from the networking device, or when it is manually taken down for maintenance.

**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>
<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 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>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.

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 (IPv4)</td>
<td>RSP3</td>
<td>Async</td>
<td>3.3</td>
<td>BGP, OSFP, ISIS, EIGRP</td>
<td>NA</td>
</tr>
<tr>
<td>64 (IPv6)</td>
<td>RSP3</td>
<td>Async</td>
<td>200</td>
<td>BGP, OSFP, ISIS, EIGRP</td>
<td>NA</td>
</tr>
<tr>
<td>64 (Software)</td>
<td>RSP3</td>
<td>BFD echo</td>
<td>3.3</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>511 (Hardware) (no client)</td>
<td>RSP3</td>
<td>BFD echo</td>
<td>3.3</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>64 (Software)</td>
<td>RSP3</td>
<td>BFD echo</td>
<td>3.3</td>
<td>BGP, OSFP, ISIS, EIGRP</td>
<td>NA</td>
</tr>
</tbody>
</table>

3 Port Channel is supported on RSP3 module in software. Minimum timer value for BFD over Port Channel is 200 ms. Hardware offload is not supported.

---

**Note**

When BFD over IPv6 is configured, the maximum scale of BFD over IPv4 reduces to 64.

**Note**

Whenever BFD discriminators are exhausted an error message “BFD discriminators exhausted. No more sessions can be created” with traceback will be printed.

**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.

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.

**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.

**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`
## Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | **enable**<br>**Example:**<br>Device> enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| 2    | **configure terminal**<br>**Example:**<br>Device# configure terminal | Enters global configuration mode. |
| 3    | **interface gigabitethernet** *number*<br>**Example:**<br>Device(config)# interface gigabitethernet 0/0/0 | Specifies the Gigabit Ethernet interface and enters interface configuration mode. |
| 4    | Perform one of the following steps:<br>• **ip address** *ipv4-address mask*<br>• **ipv6 address** *ipv6-address/mask*<br>**Example:**<br>Configuring an IPv4 address for the interface:<br>Device(config-if)# ip address 10.201.201.1 255.255.255.0<br>Configuring an IPv6 address for the interface:<br>Device(config-if)# ipv6 address 2001:db8:1:1::1/32 | Configures an IP address for the interface. |
| 5    | **bfd interval** *milliseconds min_rx milliseconds multiplier interval-multiplier*<br>**Example:**<br>Device(config-if)# bfd interval 50 min_rx 50 multiplier 5 | 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 |
| 6    | **end**<br>**Example:** | Exits interface configuration mode and returns to privileged EXEC mode. |
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]]
   [dhep] [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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: 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>Example: Device(config)# interface serial 2/0</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>4</td>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td></td>
<td>Perform one of the following steps:</td>
</tr>
<tr>
<td></td>
<td>• <code>ip address ipv4-address mask</code></td>
</tr>
<tr>
<td></td>
<td>• <code>ipv6 address ipv6-address/mask</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Configuring an IPv4 address for the interface:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <code>ip address 10.201.201.1 255.255.255.0</code></td>
</tr>
<tr>
<td></td>
<td>Configuring an IPv6 address for the interface:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <code>ipv6 address 2001:db8:1:1::1/32</code></td>
</tr>
<tr>
<td>5</td>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td></td>
<td><code>bfd interval milliseconds min_rx milliseconds interval-multiplier interval-multiplier</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <code>bfd interval 500 min_rx 500 multiplier 5</code></td>
</tr>
<tr>
<td>6</td>
<td><strong>Step 6</strong></td>
</tr>
<tr>
<td></td>
<td><code>exit</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <code>exit</code></td>
</tr>
<tr>
<td>7</td>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td></td>
<td><code>ip route static bfd interface-type interface-number ip-address [group group-name [passive]]</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <code>ip route static bfd serial 2/0 10.1.1.1 group group1 passive</code></td>
</tr>
<tr>
<td>8</td>
<td><strong>Step 8</strong></td>
</tr>
<tr>
<td></td>
<td>`ip route [vrf vrf-name] prefix mask {ip-address</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 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.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip route 10.0.0.0 255.0.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# exit</td>
<td>Exit global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>show ip static route</td>
<td>(Optional) Displays static route database information.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show ip static route</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td>show ip static route bfd</td>
<td>(Optional) Displays information about the static BFD configuration from the configured BFD groups and nongroup entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show ip static route bfd</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# exit</td>
<td>Exit privileged EXEC mode and returns to user EXEC mode.</td>
</tr>
</tbody>
</table>

---

**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"
"add no echo to template name if configured via template"
"or add no bfd echo to interface if configured"
"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>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> Switch&gt; enable</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> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> bfd slow-timer <em>milliseconds</em></td>
<td>Configures the BFD slow timer.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# bfd slow-timer 12000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits global configuration mode and returns the router to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> 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><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 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></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>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> Device&gt; enable</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> bfd-template single-hop template-name</td>
<td>Creates a BFD template and enters BFD configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
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.

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.

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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# bfd-template single-hop bfdtemplate1</td>
<td>Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD interval values that must be missed before BFD declares that a peer is unavailable.</td>
</tr>
<tr>
<td>Step 4</td>
<td>interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(bfd-config)# end</td>
</tr>
<tr>
<td>Purpose</td>
<td>Exits BFD configuration mode and returns the device to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

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.

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.

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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# bfd-template single-hop bfdtemplate1</td>
<td>Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD interval values that must be missed before BFD declares that a peer is unavailable.</td>
</tr>
<tr>
<td>Step 4</td>
<td>interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(bfd-config)# end</td>
</tr>
<tr>
<td>Purpose</td>
<td>Exits BFD configuration mode and returns the device to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code> <strong>Example:</strong> Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>bfd-template single-hop template-name</code> <strong>Example:</strong> Router(config)# bfd-template single-hop bfdtemplate1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value</code> <strong>Example:</strong> Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code> <strong>Example:</strong> Router(bfd-config)# end</td>
</tr>
</tbody>
</table>

### 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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` **Example:** Router> enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
Purpose

Command or Action

Step 2
configure terminal
Example:
Router# configure terminal

Step 3
bfd-template multi-hop template-name
Example:
Router(config)# bfd-template multi-hop mh-template1

Step 4
interval min-tx milliseconds min-rx milliseconds multiplier multiplier-value
Example:
Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3

Step 5
authentication authentication-type keychain keychain-name
Example:
Router(bfd-config)# authentication keyed-sha-1 keychain bfd-multihop

Step 6
end
Example:
Router(bfd-config)# end

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>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> 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><strong>Step 3</strong> bfd mapipv4 vrf vrf-name destination length source-address length template-name</td>
<td>Configures a BFD map and associates it with the template.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# bfd map ipv4 vrf vpn1 192.168.0.0/24 192.168.42.5/32 mh-template1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits BFD configuration mode and returns the router to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></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 RouterA 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 Gigabtethernet0/0/0
```
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 0
   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
!
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

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
OurAddr NeighAddr
LD/RD RH/RS Holdown(mult) State Int
172.16.1.1 172.16.1.3
  5/3  1(RH)  150 (3 ) Up  Gig0/0/1
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(1364284)
Rx Count: 1351813, Rx Interval (ms) min/max/avg: 28/64/49 last: 4 ms ago
Tx Count: 1364289, Tx Interval (ms) min/max/avg: 40/68/49 last: 32 ms ago
Registered protocols: EIGRP
Uptime: 18:42:45
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.: 3 - Your Discr.: 5
    Min tx interval: 50000 - Min rx interval: 50000
    Min Echo interval: 0

OurAddr NeighAddr
LD/RD RH/RS Holdown(mult) State Int
172.16.1.1 172.16.1.2
  6/1  Up  0 (3 ) Up  Gig0/0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(317)
Rx Count: 305, Rx Interval (ms) min/max/avg: 1/1016/887 last: 448 ms ago
Tx Count: 319, Tx Interval (ms) min/max/avg: 1/1008/880 last: 532 ms ago
Registered protocols: EIGRP
Uptime: 00:04:30
Last packet: Version: 1
  - Diagnostic: 0
    State bit: Up - Demand bit: 0
    Poll bit: 0 - Final bit: 0
    Multiplier: 3 - Length: 24
    My Discr.: 1 - Your Discr.: 6
    Min tx interval: 1000000 - Min rx interval: 1000000
    Min Echo interval: 50000
```

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.
RouterB# show bfd neighbors details

<table>
<thead>
<tr>
<th>OurAddr</th>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH/RS</th>
<th>Holdown(mult)</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.2</td>
<td>172.16.1.1</td>
<td>1/6</td>
<td>Up</td>
<td>0 (3)</td>
<td>Up</td>
<td>Gig0/0/1</td>
</tr>
</tbody>
</table>

Session state is UP and using echo function with 50 ms interval.

Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP

Uptime: 00:05:00

Last packet: Version: 1
- Diagnostic: 0
  - State bit: Up
  - Demand bit: 0
  - Poll bit: 0
  - Multiplier: 3
  - Length: 24
  - My Discr.: 6
  - Min tx interval: 1000000
  - Min rx interval: 1000000
  - Min Echo interval: 50000

RouterB# show bfd neighbors details

<table>
<thead>
<tr>
<th>OurAddr</th>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH/RS</th>
<th>Holdown(mult)</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.2</td>
<td>172.16.1.3</td>
<td>3/6</td>
<td>1(RH)</td>
<td>118 (3)</td>
<td>Up</td>
<td>Gig0/0/1</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
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
  - Multiplier: 3
  - Length: 24
  - My Discr.: 6
  - 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

<table>
<thead>
<tr>
<th>OurAddr</th>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH/RS</th>
<th>Holdown(mult)</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.1</td>
<td>172.16.1.3</td>
<td>5/3</td>
<td>1(RH)</td>
<td>134 (3)</td>
<td>Up</td>
<td>Gig0/0/1</td>
</tr>
</tbody>
</table>
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 123
  log-adjacency-changes detail
  network 172.16.0.0 0.0.0.255 area 0
  network 172.17.0.0 0.0.0.255 area 0
  bfd all-interfaces
```

**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 ospf 123
  log-adjacency-changes detail
  network 172.16.0.0 0.0.0.255 area 0
  network 172.18.0.0 0.0.0.255 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.
The output from the `show bfd neighbors details` command from 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: 10000, Multiplier: 3
Received MinRxInt: 10000, Received Multiplier: 5
Holdown (hits): 10126, Rx Interval (ms) min/max/avg: 152/440/332 last: 12 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
    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 Adj s 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.

```
RouterA# show ospf
```

---

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

---

**Bidirectional Forwarding Detection**

**Example: Configuring BFD in an OSPF Network**
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
No backup designated router on this network
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

```plaintext
! 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
 bpg 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

```plaintext
! 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
 bpg 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

<table>
<thead>
<tr>
<th>OurAddr</th>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH</th>
<th>Holdown(mult)</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.1</td>
<td>172.16.10.2</td>
<td>1/8</td>
<td>1</td>
<td>332 (3 )</td>
<td>Up</td>
<td>Gig0/0/1</td>
</tr>
</tbody>
</table>

Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(15491)
Rx Count: 9160, Rx Interval (ms) min/max/avg: 200/440/332 last: 268 ms ago
Tx Count: 15494, Tx Interval (ms) min/max/avg: 152/248/197 last: 32 ms ago

Registered protocols: BGP

Uptime: 00:50:45
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.: 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 on Router B verifies that a BFD session has been created:

Router B

Router> show bfd neighbors details

Cleanup timer hits: 0

<table>
<thead>
<tr>
<th>OurAddr</th>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH</th>
<th>Holdown(mult)</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.2</td>
<td>172.16.10.1</td>
<td>8/1</td>
<td>1</td>
<td>1000 (5 )</td>
<td>Up</td>
<td>Gig0/0/0</td>
</tr>
</tbody>
</table>

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: 5996, 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
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 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
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
```
### 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.

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.

```plaintext
<table>
<thead>
<tr>
<th>OurAddr</th>
<th>NeighAddr</th>
<th>LD/RD RH</th>
<th>Holdown(mult)</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.1</td>
<td>172.16.10.2</td>
<td>1/8</td>
<td>1</td>
<td>536 (3)</td>
<td>Up</td>
</tr>
</tbody>
</table>

Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(23543)
Rx 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:

```plaintext
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr | NeighAddr | LD/RD RH | Holdown(mult) | State  | Int  |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.2</td>
<td>172.16.10.1</td>
<td>8/1</td>
<td>1</td>
<td>1000 (5)</td>
<td>Up</td>
</tr>
</tbody>
</table>

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
  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 Adjs Found: 1
```
**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

**Router B**

interface GigabitEthernet0/0/1
  ip address 10.1.0.22 255.255.0.0
  no shutdown
  bfd interval 200 min_rx 200 multiplier 3
  standby 1 ip 10.0.0.11
  standby 1 preempt
  standby 1 priority 90
  standby 2 ip 10.0.0.12
  standby 2 preempt
  standby 2 priority 80

The output from the `show standby neighbors` command verifies that a BFD session has been created:

RouterA# show standby neighbors
HSRP neighbors on GigabitEthernet0/0/0
  10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled!
RouterB# show standby neighbors
HSRP neighbors on GigabitEthernet0/0/1
  10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled!

**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
```
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 10.1.1.1 255.255.255.255 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 GigabitEthernet 0/0/0 209.165.200.225

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 GigabitEthernet 0/0/0 209.165.200.225
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
Static Route Support for BFD over IPv6

- Restrictions for Static Route for BFD over IPv6, on page 35
- Information About Static Route Support for BFD over IPv6, on page 35
- How to Configure Bidirectional Forwarding Detection for IPv6, on page 36
- Configuration Examples for Static Route Support for BFD over IPv6, on page 38

Restrictions for Static Route for BFD over IPv6

- Multi-hop is not supported for static route.
- BFD over IPv6 is not supported on the ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.

Information About Static Route Support for BFD over IPv6

Using the BFDv6 protocol to reach the static route next hop ensures that an IPv6 static route is inserted only in the IPv6 Routing Information Base (RIB) when the next-hop neighbor is reachable. Using the BFDv6 protocol also can remove the IPv6 static route from the IPv6 RIB when the next hop becomes unreachable.

A user can configure IPv6 static BFDv6 neighbors. These neighbor can operate in one of two modes: associated (which is the default) and unassociated. A neighbor can be transitioned between the two modes without interrupting the BFDv6 session associated with the neighbor.

BFDv6 Associated Mode

In Bidirectional Forwarding Detection for IPv6 (BFDv6) associated mode, an IPv6 static route is automatically associated with an IPv6 static BFDv6 neighbor if the static route next hop exactly matches the static BFDv6 neighbor.

An IPv6 static route requests a BFDv6 session for each static BFDv6 neighbor that has one or more associated IPv6 static routes and is configured over an interface on which BFD has been configured. The state of the BFDv6 session will be used to determine whether the associated IPv6 static routes are inserted in the IPv6 RIB. For example, static routes are inserted in the IPv6 RIB only if the BFDv6 neighbor is reachable, and the static route is removed from the IPv6 RIB if the BFDv6 neighbor subsequently becomes unreachable.

BFDv6 associated mode requires you to configure a BFD neighbor and static route on both the device on which the BFD-monitored static route is required and on the neighboring device.
**BFDv6 Unassociated Mode**

An IPv6 static BFD neighbor may be configured as unassociated. In this mode, the neighbor is not associated with static routes, and the neighbor always requests a BFDv6 session if the interface has been configured for BFDv6.

Unassociated mode is useful in the following situations:

- Bringing up a BFDv6 session in the absence of an IPv6 static route—This case occurs when a static route is on router A, with router B as the next hop. Associated mode requires you to create both a static BFD neighbor and static route on both routers in order to bring up the BFDv6 session from B to A. Specifying the static BFD neighbor in unassociated mode on router B avoids the need to configure an unwanted static route.

- Transition to BFD monitoring of a static route—This case occurs when existing IPv6 static routes are inserted in the IPv6 RIB. Here, you want to enable BFD monitoring for these static routes without any interruption to traffic. If you configure an attached IPv6 static BFD neighbor, then the static routes will immediately be associated with the new static BFD neighbor. However, because a static BFD neighbor starts in a down state, the associated static routes are then removed from the IPv6 RIB and are reinserted when the BFDv6 session comes up. Therefore, you will see an interruption in traffic. This interruption can be avoided by configuring the static BFD neighbor as unassociated, waiting until the BFDv6 session has come up, and then reconfiguring the static BFD neighbor as associated.

- Transition from BFD monitoring of a static route—In this case, IPv6 static routes are monitored by BFD and inserted in the RIB. Here, you want to disable BFD monitoring of the static routes without interrupting traffic flow. This scenario can be achieved by first reconfiguring the static BFD neighbor as detached (thus disassociating the neighbor from the static routes) and then deconfiguring the static BFD neighbor.

**How to Configure Bidirectional Forwarding Detection for IPv6**

**Specifying a Static BFDv6 Neighbor**

An IPv6 static BFDv6 neighbor is specified separately from an IPv6 static route. An IPv6 static BFDv6 neighbor must be fully configured with the interface and neighbor address and must be directly attached to the local router.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ipv6 route static bfd [vrf vrf-name] interface-type interface-number ipv6-address [unassociated]`

**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>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Associating an IPv6 Static Route with a BFDv6 Neighbor

IPv6 static routes are automatically associated with a static BFDv6 neighbor. A static neighbor is associated with a BFDv6 neighbor if the static next-hop explicitly matches the BFDv6 neighbor.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ipv6 route static bfd [vrf vrf-name] interface-type interface-number ipv6-address [unassociated]`
4. `ipv6 route [vrf vrf-name] ipv6-prefix /prefix-length [ipv6-address | interface-type interface-number ipv6-address] [nexthop-vrf [vrf-name | default]] [administrative-distance] [administrative-multicast-distance | unicast | multicast] [next-hop-address] [tag tag]`

**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></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**                                                 |         |
| configure terminal                                         | Enters global configuration mode. |
| Example:                                                   |         |
| Device# configure terminal                                 |         |

| **Step 3**                                                 |         |
| ipv6 route static bfd [vrf vrf-name] interface-type interface-number ipv6-address [unassociated] | Specifies static route BFDv6 neighbors. |
| Example:                                                   |         |
| Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1 |         |
### Command or Action

**Step 4**

```
ipv6 route [vrf vrf-name] ipv6-prefix / prefix-length
{ipv6-address | interface-type interface-number
ipv6-address}] [nexthop-vrf [vrf-name1 | default]]
[administrative-distance] [administrative-multicast-distance
| unicast | multicast] [next-hop-address] [tag tag]
```

**Example:**

```
Device(config)# ipv6 route 2001:DB8::/64
gigabitethernet 0/0/0 2001::1
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Establishes static IPv6 routes.</td>
</tr>
</tbody>
</table>

### Configuration Examples for Static Route Support for BFD over IPv6

#### Example: Specifying an IPv6 Static BFDv6 Neighbor

The following example specifies a fully configured IPv6 static BFDv6 neighbor. The interface is GigabitEthernet 0/0/0 and the neighbor address is 2001::1.

```
Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1
```

#### Example: Associating an IPv6 Static Route with a BFDv6 Neighbor

In this example, the IPv6 static route 2001:DB8::/32 is associated with the BFDv6 neighbor 2001::1 over the GigabitEthernet 0/0/0 interface:

```
Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1
Device(config)# ipv6 route 2001:DB8::/32 gigabitethernet 0/0/0 2001::1
```
BFD on BDI Interfaces

The Cisco BFD on BDI Interfaces feature alleviates limitations on the maximum number of interfaces per system that switched virtual interfaces (SVI) impose. This document describes how to configure the Bidirectional Forwarding Detection (BFD) protocol on bridge domain interfaces (BDIs).

- Information About BFD on Bridge Domain Interfaces, on page 39
- How to Configure BFD on BDI Interfaces, on page 39
- Configuration Examples for BFD on BDI Interfaces, on page 42

Information About BFD on Bridge Domain Interfaces

BFD on Bridge Domain Interfaces

Each BDI is associated with a bridge domain on which traffic is mapped using criteria defined and configured on the associated Ethernet flow points (EFPs). You can associate either single or multiple EFPs with a given bridge domain. Thus you can establish a BFD single-hop session over BDI interfaces that are defined in either a global table or a VPN routing and forwarding (VRF) table, and all existing single-hop BFD clients will be supported for BFD over BDI.

The Cisco BFD on BDI feature does not affect BFD stateful switchover (SSO) on platforms that are SSO capable.

How to Configure BFD on BDI Interfaces

Enabling BFD on a Bridge Domain Interface

Perform these steps to enable single hop BFD on an individual BDI interface.

Note

Multihop BFD is not interface specific so you do not need BDI interface-level configuration to establish multihop BFD sessions.
**Before you begin**

Two or more nodes must be connected.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. ip address ip-address mask
5. bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier
6. exit

**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></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</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></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures a bridge domain interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface bdi 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address ip-address mask</td>
<td>Configures an IP address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 10.201.201.1 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</td>
<td>Enables BFD on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(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></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Associating an Ethernet Flow Point with a Bridge Domain

**Before you begin**

BFD must be enabled on both nodes.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/subslot/port
4. no ip address
5. negotiation auto
6. cdp enable
7. service instance id service-type
8. encapsulation dot1q vlan-id
9. rewrite ingress tag pop 1 symmetric
10. exit
11. exit
12. bridge-domain vlan-id

**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>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/subslot/port</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# interface GigabitEthernet0/0/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no ip address</td>
<td>Disables IP processing.</td>
</tr>
<tr>
<td>Example: Router(config-if)# no ip address</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> negotiation auto</td>
<td>Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the interface.</td>
</tr>
<tr>
<td>Example: Router(config-if)# negotiation auto</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>cdp enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# cdp enable</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>service instance id service-type</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# service instance 2 ethernet</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>encapsulation dot1q vlan-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if-srv)# encapsulation dot1q 2</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>rewrite ingress tag pop 1 symmetric</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if-srv)# rewrite ingress tag pop 1 symmetric</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# exit</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# exit</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>bridge-domain vlan-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# bridge-domain 2</td>
</tr>
</tbody>
</table>

**What to do next**

**Configuration Examples for BFD on BDI Interfaces**

**Examples for BFD on BDI Interfaces**

The following example shows how to configure BFD on a BDI.
BFD on BDI Interfaces

Examples for BFD on BDI Interfaces

Router#show bfd neighbors

<table>
<thead>
<tr>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH/RS</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.2</td>
<td>2049/1</td>
<td>Up</td>
<td>Up</td>
<td>BD2</td>
</tr>
</tbody>
</table>

Router# show running interface gi0/0/3

Current configuration : 230 bytes

interface GigabitEthernet0/0/3
no ip address
ip pim passive
ip igmp version 3
negotiation auto
cdp enable
service instance 2 ethernet
   encapsulation dot1q 2
   rewrite ingress tag pop 1 symmetric
   bridge-domain 2
!
end

Router# show running interface bdi2

Current configuration : 127 bytes

interface BDI2
ip address 10.1.1.3 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3
bfd neighbor ipv4 10.1.1.2
end

And similarly for the other node:

Router2# show running interface bdi2

Current configuration : 127 bytes

interface BDI2
ip address 10.1.1.2 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3
bfd neighbor ipv4 10.1.1.3
end

ED3# show int gig0/0/3

Current configuration : 195 bytes

interface GigabitEthernet0/0/3
no ip address
negotiation auto
cdp enable
service instance 2 ethernet
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
bridge-domain 2
!
end

Router2#show bfd neighbors

IPv4 Sessions
NeighAddr   LD/RD   RH/RS  State  Int
10.1.1.3    1/2049  Up      Up      BD2
ED3#
IS-IS IPv6 Client for BFD

When Bidirectional Forwarding Detection (BFD) support is configured with Intermediate System To Intermediate System (IS-IS) as a registered protocol with BFD, IS-IS receives forwarding path detection failure messages from BFD.

- Prerequisites for IS-IS IPv6 Client for BFD, on page 45
- Restrictions for IS-IS IPv6 Client for BFD, on page 45
- Information About IS-IS IPv6 Client for BFD, on page 45
- How to Configure ISIS IPv6 Client for BFD, on page 46
- Configuration Examples for ISIS IPv6 Client for BFD, on page 48

Prerequisites for IS-IS IPv6 Client for BFD

- IS-IS must be running on all participating devices.
- The baseline parameters for BFD sessions must be configured on the interfaces that run BFD sessions to BFD neighbors.

Restrictions for IS-IS IPv6 Client for BFD

- Only one IS-IS IPv6 session is supported.
-Ipv6 for BFD client is not supported on the ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.

Information About IS-IS IPv6 Client for BFD

IS-IS BFD Topology

When BFD support is configured with IS-IS as a registered protocol with BFD, IS-IS receives forwarding path detection failure messages from BFD. BFD support for IS-IS can be configured in either router address-family configuration mode or interface configuration mode. IS-IS IPv6 can run in single-topology or in Multi-Topology (MT) mode.
IS-IS BFD supports both IPv4 and IPv6 on the same adjacency for single-topology or multi-topology mode. If BFD is enabled for both IPv4 and IPv6, IS-IS sends two BFD session creation requests to BFD. For single-topology mode, the IS-IS adjacency state can only be UP if both BFD sessions are UP. If either of the BFD sessions is DOWN, the associated IS-IS adjacency state is also DOWN. For MT mode, the IS-IS adjacency state can be UP as long as one of topologies has a BFD session in an UP state.

**IS-IS BFD IPv6 Session Creation**

IS-IS requests a BFD session for the interface and IPv6 address of the neighboring device when all of the following conditions are met:

- An IS-IS adjacency entry exists.
- The Address Family Identifier (AFI) specific peer interface address is known.
- IS-IS BFD is enabled for that AFI on an interface.
- IS-IS is enabled for that AFI on the local interface.
- If the neighboring device supports RFC 6213, BFD must be enabled for the specified Multi-Topology Identifier (MTID) or Network Layer Protocol Identifier (NLPID).

**IS-IS BFD IPv6 Session Deletion**

When IS-IS BFD IPv6 is disabled on an interface, IS-IS removes related BFD sessions for IPv6 from the adjacent device. When the IS-IS adjacency entry is deleted, all BFD sessions are also deleted. IS-IS requests BFD to remove each BFD session that it has requested when any of the following events occur:

- The IS-IS instance is deleted or un-configured.
- The IS-IS adjacency entry is deleted.
- IS-IS BFD is disabled on the next hop interface for an address-family.
- The neighboring device supports RFC 6213 and indicates that it no longer supports BFD for the specified MTID or NLPID.

**How to Configure ISIS IPv6 Client for BFD**

**Configuring IS-IS IPv6 Client Support for BFD on an Interface**

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `isis ipv6 bfd`
5. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>enable</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

* • Enter your password if prompted.

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>interface type number</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# interface gigabitethernet 6/0/0</td>
<td>Enters interface configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>isis ipv6 bfd</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-if)# isis ipv6 bfd</td>
<td>Enables IPv6 BFD on a specific interface that is configured for IS-IS.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-if)# end</td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

## Configuring IS-IS IPv6 Client Support for BFD on All Interfaces

### SUMMARY STEPS

1. enable
2. configure terminal
3. router isis
4. metric-style wide
5. address-family ipv6
6. multi-topology
7. bfd all-interfaces
8. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>enable</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

* • Enter your password if prompted.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>router isis</td>
<td>Enables the IS-IS routing protocol and enters router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# router isis</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>metric-style wide</td>
<td>(Optional) Configures a device that is running IS-IS so that it generates and accepts only new-style type, length, value objects (TLVs).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-router)# metric-style wide</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>address-family ipv6</td>
<td>Enters address family configuration mode for configuring IS-IS routing sessions that use standard IPv6 address prefixes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-router)# address-family ipv6</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-router-af)# multi-topology</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>bfd all-interfaces</td>
<td>Enables BFD for all interfaces participating in the routing process.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-router-af)# bfd all-interfaces</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Exits address family configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-router-af)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Examples for ISIS IPv6 Client for BFD**

**Example: IS-IS IPv6 Client Support for BFD on a Single Interface**

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 6/0/0
```
Example: IS-IS IPv6 Client Support for BFD on All Interfaces

Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 6/0
Device(config-if)# isis ipv6 bfd
Device(config-if)# end

Device(config)# router isis
Device(config-router)# metric-style wide
Device(config-router)# address-family ipv6
Device(config-router-af)# multi-topology
Device(config-router-af)# bfd all-interfaces
Device(config-router-af)# end
Example: IS-IS IPv6 Client Support for BFD on All Interfaces
BFD IPv6 Encapsulation Support

Bidirectional Forwarding Detection for IPv6 encapsulations are described within a session information structure. These session information structures are defined by BFDv6 for the protocols supported. BFDv6 uses information from the session information structures to determine the correct encapsulation for BFDv6 packets on that session.

- Prerequisites for BFD IPv6 Encapsulation Support, on page 51
- Restrictions for BFD IPv6 Encapsulation Support, on page 51
- Information About BFD IPv6 Encapsulation Support, on page 51
- How to Configure BFD IPv6 Encapsulation Support, on page 53
- Configuration Examples for BFD IPv6 Encapsulation Support, on page 54

Prerequisites for BFD IPv6 Encapsulation Support

When using Bidirectional Forwarding Detection over IPv6 (BFDv6), IPv6 Cisco Express Forwarding and IPv6 unicast routing must be enabled on all participating routers.

Restrictions for BFD IPv6 Encapsulation Support

- BFDv6 supports only global IPv6 neighbor addresses if a global IPv6 address is configured on the interface.
- Only asynchronous mode is supported. In asynchronous mode, either BFDv6 peer can initiate a BFDv6 session.
- BFDv6 is not supported on the ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.

Information About BFD IPv6 Encapsulation Support

Overview of the BFDv6 Protocol

This section describes the BFDv6 protocol, how it is different from BFD for IPv4, and how it works with BFD for IPv4. BFD is a detection protocol designed to provide fast forwarding path failure detection times
for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. BFDv6 provides IPv6 support by accommodating IPv6 addresses and provides the ability to create BFDv6 sessions.

**BFDv6 Registration**

BFD clients register with BFD using a registry application program interface (API). The registry arguments include protocol type and the address and interface description block (IDB) of the route to be monitored. These APIs and arguments are all assumed by BFD to be IPv4.

BFDv6 has registries from which these arguments have been removed, and the protocol and encapsulation are described within a session information structure. These session information structures are defined by BFDv6 for the protocols supported. BFDv6 uses information from the session information structures to determine the correct encapsulation for BFDv6 packets on that session.

**BFDv6 Global and Link-Local Addresses**

BFDv6 supports both global and link-local IPv6 addresses for neighbor creation. BFDv6 sessions select source addresses to match the neighbor address types (for example, global IPv6 address neighbors must be paired with global IPv6 source addresses and link-local IPv6 address neighbors must be paired with link-local IPv6 source addresses). The table below shows the address pairings that BFDv6 supports.

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Global</td>
<td>Supported</td>
</tr>
<tr>
<td>Global</td>
<td>Link local</td>
<td>Not supported</td>
</tr>
<tr>
<td>Link local</td>
<td>Global</td>
<td>Not supported</td>
</tr>
<tr>
<td>Link local</td>
<td>Link local</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Because all IPv6-enabled interfaces have a link-local address and BFDv6 selects the source address, link-local address neighbors are always paired with a link-local interface address. The link-local source address with global destination address is not supported by Cisco Express Forwarding. Therefore, a global IPv6 address must be configured on an interface before a session with a global address neighbor may be established in BFDv6. BFDv6 rejects any sessions in which the neighbor address is global and no global address is configured on the interface.

---

**Note**

The behavior of a unique local address (ULA) in BFDv6 is the same as a global address.

**BFD for IPv4 and IPv6 on the Same Interface**

BFD supports multiple IPv4 and IPv6 sessions per interface, with no restriction on the protocol of those sessions.
How to Configure BFD IPv6 Encapsulation Support

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.

**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.

**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

**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.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface gigabitethernet number</td>
<td>Specifies the Gigabit Ethernet interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface gigabitethernet 0/0/0</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Perform one of the following steps: • ip address ipv4-address mask</td>
<td>Configures an IP address for the interface.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>• ipv6 address ipv6-address/mask</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Configuring an IPv4 address for the interface:</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip address 10.201.201.1 255.255.255.0</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Configuring an IPv6 address for the interface:</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ipv6 address 2001:db8:1:1::1/32</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# bfd interval 50 min_rx 50 multiplier 5</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# end</td>
<td>Enables BFD on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples for BFD IPv6 Encapsulation Support

#### Example: Configuring BFD Session Parameters on the Interface

Device# show ipv6 ospf neighbor detail

Neighbor 172.16.3.3
In the area 1 via interface GigabitEthernet0/0/0
Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
Neighbor priority is 1, State is FULL, 6 state changes
DR is 172.16.6.6 BDR is 172.16.3.3
Options is 0x63F813E9
Dead timer due in 00:00:33
Neighbor is up for 00:09:00
Index 1/1/2, retransmission queue length 0, number of retransmission 2
Last retransmission scan length is 1, maximum is 2
Last retransmission scan time is 0 msec, maximum is 0 msec
Configuring BFD Debug Enhancement

The Bidirectional Forwarding Detection (BFD) Debug Enhancement feature enables logging of debugging information for critical BFD events, normal BFD events, and BFD packets. This feature enables BFD event traces and BFD event logs. This feature allows network engineers and operators to easily identify and analyze issues with BFD sessions.

- Finding Feature Information, on page 57
- Prerequisites for BFD Debug Enhancement, on page 57
- Restrictions for BFD Debug Enhancement, on page 57
- Information About BFD Debug Enhancement, on page 58
- How to Configure BFD Debug Enhancement, on page 58
- Configuration Examples for BFD Debug Enhancement, on page 60
- Additional References for BFD Debug Enhancement, on page 61
- Feature Information for BFD Debug Enhancement, on page 62

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for BFD Debug Enhancement

Bidirectional Forwarding Detection (BFD) feature must be running on the device.

Restrictions for BFD Debug Enhancement

The Bidirectional Forwarding Detection (BFD) event trace logs cannot store more than 65536 elements in a BFD instance. Once the log elements reach this limit, new log entries replace the old log entries.

RSP3 do not support the Bidirectional Forwarding Detection (BFD) debug enhancement.
Information About BFD Debug Enhancement

Overview of BFD Debug Enhancement

The Bidirectional Forwarding Detection (BFD) Debug Enhancement feature enables logging of debugging information for critical BFD events, normal BFD events, and BFD packets. This feature enables BFD event traces and BFD event logs.

BFD Debug Enhancement - Event Tracer subsystem

The Event Tracer subsystem in the BFD Debug Enhancement feature helps network engineers trace BFD events. This subsystem generates debugging information that can be extracted and analyzed. You can optionally store the traced data in a file for further analysis.

BFD Debug Enhancement - Event Log Architecture

The Event Log Architecture in the BFD Debug Enhancement feature is classified into three types:

- **BFD Critical**—Logs debugging information about all critical BFD event traces, whenever the BFD session attains the DOWN state.
- **BFD Event**—Logs debugging information about all BFD events that can be logged using the `debug bfd event` command.
- **BFD Packet**—Logs debugging information about all BFD packets that can be logged using the `debug bfd packet` command.

How to Configure BFD Debug Enhancement

Configuring BFD Debug Enhancement

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet number`
4. `bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier`
5. `end`
6. `debug bfd event`
7. `debug bfd packet`
8. `monitor event-trace bfd event enable`
9. `monitor event-trace bfd event all enable`
10. `monitor event-trace bfd packet enable`
11. `monitor event-trace bfd packet all enable`
12. `show monitor event-trace bfd`
## 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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong></td>
<td>Specifies the Gigabit Ethernet interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>interface gigabitethernet <em>number</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device(config)# interface gigabitethernet 0/0/0</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong></td>
<td>Enables Bidirectional Forwarding Detection (BFD) on the interface.</td>
</tr>
<tr>
<td></td>
<td>bfd interval <em>milliseconds min_rx milliseconds multiplier interval-multiplier</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device(config-if)# bfd interval 50 min_rx 50 multiplier 5</td>
</tr>
<tr>
<td></td>
<td><strong>Step 5</strong></td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>end</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device(config-if)# end</td>
</tr>
<tr>
<td></td>
<td><strong>Step 6</strong></td>
<td>Enables debugging information for BFD events.</td>
</tr>
<tr>
<td></td>
<td>debug bfd event</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device# debug bfd event</td>
</tr>
<tr>
<td></td>
<td><strong>Step 7</strong></td>
<td>Enables debugging information for BFD packets.</td>
</tr>
<tr>
<td></td>
<td>debug bfd packet</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device# debug bfd packet</td>
</tr>
<tr>
<td></td>
<td><strong>Step 8</strong></td>
<td>Enables the event traces for normal BFD events.</td>
</tr>
<tr>
<td></td>
<td>monitor event-trace bfd event enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device# monitor event-trace bfd event enable</td>
</tr>
<tr>
<td></td>
<td><strong>Step 9</strong></td>
<td>Enables the event trace filters for normal BFD events.</td>
</tr>
<tr>
<td></td>
<td>monitor event-trace bfd event all enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device# monitor event-trace bfd event all enable</td>
</tr>
<tr>
<td></td>
<td><strong>Step 10</strong></td>
<td>Enables the event traces for BFD packet events.</td>
</tr>
<tr>
<td></td>
<td>monitor event-trace bfd packet enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Device# monitor event-trace bfd packet enable</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 11**

*monitor event-trace bfd packet all enable*

**Example:**

Device# monitor event-trace bfd packet all enable

**Purpose**

Enables the event trace filters for BFD packet events.

**Step 12**

*show monitor event-trace bfd*

**Example:**

Device# show monitor event-trace bfd

**Purpose**

Displays event trace messages for BFD events. Use the `critical`, `event`, and `packet` keywords to display event trace messages for critical BFD events, normal BFD events, and BFD packet events, respectively.

### Configuration Examples for BFD Debug Enhancement

#### Example: Configuring BFD Debug Enhancement

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# bfd interval 50 min_rx 50 multiplier 5
Device(config-if)# end
Device# debug bfd event
Device# debug bfd packet
Device# monitor event-trace bfd event enable
Device# monitor event-trace bfd event all enable
Device# monitor event-trace bfd packet enable
Device# monitor event-trace bfd packet all enable
Device# show monitor event-trace bfd critical all
Device# show monitor event-trace bfd event all
Device# show monitor event-trace bfd packet all
```

The following is sample output from the *show monitor event-trace bfd* command for a critical BFD event:

```
Oct 2 10:57:25.173: BFD-DEBUG CRITICAL: V1 FSM ld:1 handle:1
Event:DETECT TIMER EXPIRED state:UP Rx Count:123 Tx Count: 120
Echo Rx:[-][-][-]
Echo Tx:[-][-][-]
```

The following is sample output from the *show monitor event-trace bfd* command for a normal BFD event:

```
Oct 2 10:57:25.173: BFD-DEBUG CRITICAL: V1 FSM ld:1 handle:1
Event:ECHO FAILURE state:UP Rx Count:123 Tx Count: 120
```

The following is sample output from the *show monitor event-trace bfd* command for a critical BFD event:

```
Oct 2 10:57:25.273: BFD-DEBUG CRITICAL: V1 FSM ld:1 handle:1
Event:ECHO FAILURE state:UP Rx Count:123 Tx Count: 120
```
Logs all events that are logged using the `debug bfd event` command.

```
Device# show monitor event-trace bfd event latest
```

The following is sample output from the `show monitor event-trace bfd` command for a BFD packet event:

```
Log all packet events that are logged using the `debug bfd packet` command.

```
Device# show monitor event-trace bfd packet latest
*Oct 12 05:30:46.849: BFD-DEBUG Packet: Tx IP:10.1.1.2 ld/rd:1/0
diag:7(Administratively Down) AdminDown  cnt:21 (0)
```

## Additional References for BFD Debug Enhancement

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Commands</td>
<td>IP Routing Protocol-Independent Commands A through R</td>
</tr>
<tr>
<td></td>
<td>IP Routing Protocol-Independent Commands S through T</td>
</tr>
<tr>
<td>Cisco IOS Commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>
Technical Assistance

**Description**
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

**Link**
http://www.cisco.com/support

### Feature Information for BFD Debug Enhancement

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Table 5: Feature Information for BFD Debug Enhancement

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Debug Enhancement</td>
<td>Cisco IOS XE Release 3.10S</td>
<td>The Bidirectional Forwarding Detection (BFD) Debug Enhancement feature enables logging of debugging information for critical BFD events, normal BFD events, and BFD packets. This feature enables BFD event traces and BFD event logs. The following commands were introduced: <code>monitor event-trace bfd</code>, <code>monitor event-trace bfd event</code>, <code>monitor event-trace bfd packet</code>, and <code>show monitor event-trace bfd</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Bidirectional Forwarding Detection Configuration of Deterministic Hardware Offload

This chapter provides information about configuring the Bidirectional Forwarding Detection (BFD) deterministic hardware offload feature on the router.

Prerequisites for BFD Deterministic Hardware Offload

- This feature must be deployed only after identifying a downtime.

Restrictions for BFD Deterministic Hardware Offload

- For existing BFD sessions (before using a new configuration command) to be made deterministic, you must recreate the sessions using the `shutdown` or `no shutdown` command, or reconfigure them.
- BFD echo with uRPF is not supported on the router for both hardware and software based BFD sessions.
- Echo based sessions—Maximum supported in hardware is 255.
- Non-echo based sessions—Maximum supported in hardware is 511.

Hardware offload BFD Echo Sessions on RSP3 Module

- Packets may get punted to CPU for hardware offload per sessions, when the BFD template is removed and added. This issue occurs on the RSP3 module with 1K BFD sessions using the same template. Some software BFD sessions might flap due to this issue.
- Hardware offloaded BFD echo packets are not punted to the ICMP queue, hence ICMP redirects are not generated.

Hardware offload BFD Echo Sessions on RSP2 Module

BFD echo packet with the same source and destination IP address are punted to the ICMP queue. This generates ICMP redirects.

- Information About BFD Deterministic Hardware Offload, on page 66
- Configuring BFD Deterministic Hardware Offload, on page 66
- Example for Configuring BFD Deterministic Hardware Offload, on page 67
Information About BFD Deterministic Hardware Offload

The BFD deterministic hardware offload feature allows you to define the BFD transmission timer value. Any BFD sessions below or equal to the set value are sent to hardware. In the conventional BFD design, sessions can be hosted in hardware or software. However, sessions hosted in hardware have the advantage of running at more aggressive timers and not being impacted by CPU spikes.

Currently the determination of which session is hosted in hardware or software is done on a first come first serve basis. The sessions are hosted in hardware till the hardware limit is reached and then the sessions are either hosted in software (if supported) or rejected. In addition, after stateful switchover (SSO) or on reloading, sessions which are hosted in hardware do not necessarily remain in hardware. A similar condition applies for software sessions. The number of BFD sessions that can be supported in the hardware are also limited.

The BFD deterministic hardware offload feature allows you to select the destination of sessions to either hardware or software. This feature allows sessions hosted in hardware to remain in hardware after SSO or reload.

Using this feature you can configure a global command which defines the BFD transmission timer below or equal to the sessions are hosted in hardware.

Note
On reaching hardware session limit, inactive BFD session do not come up when an active session is removed.

Note
Starting with Cisco IOS XE Release 3.13, the global command defines the BFD transmission timer below which the sessions are hosted in hardware; those equal to or above this value are hosted in the software.

Configuring BFD Deterministic Hardware Offload

To set the timer value below which the BFD sessions are offloaded to hardware, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. platform bfd-offload-timer timervalue
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>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 2** | **configure terminal**
*Example:*
Router# configure terminal | Enters global configuration mode.

**Step 3** | **platform bfd-offload-timer** *timervalue*
*Example:*
Router(config)# platform bfd-offload-timer 5000 | Sets the timer value.

- *timervalue*—The valid range is from 200000-999000 microseconds.

**Note** There is no default value for this timer. The timer is enabled only after you specify a valid non-zero value. Starting with Cisco IOS Release 3.13, the timer value range is from 200000-999000 microseconds. For releases prior to Cisco IOS Release 3.13, the timer value range is 3300-999000 microseconds.

**Step 4** | **end**
*Example:*
Router(config)# end | Exits interface configuration mode and returns to privileged EXEC mode.

---

**Example for Configuring BFD Deterministic Hardware Offload**

The following example shows how to set the timer value to 400 microseconds:

Router> enable
Router# configure terminal
Router(config)# platform bfd-offload-timer 400000
Router(config)# end

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidirectional Forwarding Detection</td>
<td>Cisco IOS Software Releases 12.2 SX Bidirectional Forwarding Detection</td>
</tr>
</tbody>
</table>

**Standards**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Title</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
INDEX

T

topic 65