



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.

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Bidirectional Forwarding Detection, on page 1](#)
- [Restrictions for Bidirectional Forwarding Detection, on page 2](#)
- [Information About Bidirectional Forwarding Detection, on page 3](#)
- [How to Configure Bidirectional Forwarding Detection, on page 8](#)
- [Configuration Examples for Bidirectional Forwarding Detection, on page 32](#)
- [Additional References, on page 51](#)
- [Feature Information for Bidirectional Forwarding Detection, on page 53](#)

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 Bidirectional Forwarding Detection

- Cisco Express Forwarding and IP routing must be enabled on all participating routers.
- One of the IP routing protocols supported by BFD must be configured on the routers before BFD is deployed. You should implement fast convergence for the routing protocol that you are using. See the IP routing documentation for your version of Cisco IOS software for information on configuring fast

convergence. See the Restrictions for Bidirectional Forwarding Detection section for more information on BFD routing protocol support in Cisco IOS software.

Restrictions for Bidirectional Forwarding Detection

- When BFD is enabled on an interface, an ACL with "log" keyword is not supported on that interface.
- Object-based ACL is not supported on BFD-enabled interface.
- The Cisco IOS software incorrectly allows configuration of BFD on virtual-template and dialer interfaces; however, BFD functionality on virtual-template and dialer interfaces is not supported. Avoid configuring BFD on virtual-template and dialer interfaces.
- BFD is supported on point-to-point IPsec tunnel.
- BFD support is not available for all platforms and interfaces. To confirm BFD support for a specific platform or interface and obtain the most accurate platform and hardware restrictions, see the Cisco IOS software release notes for your software version.
- BFD packets are not matched in the QoS policy for self-generated packets.
- BFD packets are matched in the **class class-default** command. So, the user must make sure of the availability of appropriate bandwidth to prevent dropping of BFD packets due to oversubscription.
- BFD between peers goes down when the entry for the BFD control packets in the applied interface ACL has log keyword added as shown in the below example:

```
10 permit ip 10.255.255.0 0.0.0.255 10.255.255.0 0.0.0.255 log
```

This behavior is seen both in echo and nonecho mode, with BFD templates also. Change in timers does not change the behavior. Any value below 750 milliseconds makes the BFD go down, 750 milliseconds 1000 milliseconds results in constant flapping of BFD and from 1000 milliseconds.

- Users have to destroy BFD session on both shut down and no shut down interfaces when a switch happens on the BFD Echo and None-Echo mode.
- The use of echo mode for single-hop BFD sessions on unnumbered interfaces is unreliable and may result in inability to properly detect failures. It is strongly recommended that echo mode be disabled when using single hop BFD on unnumbered interfaces. See [Example: Disabling Echo Mode When Configuring Single-Hop BFD on Unnumbered Interfaces](#), on page 51.
- When configuring BFD over Bundle Interface, the BFD timer should be larger than 750*3 milliseconds and the carrier delay time must be configured as 0 on the physical interface, using the "carrier-delay 0" command in interface configuration.

Support for Point-to-Point IPv4, IPv6, and GRE Tunnels

Depending on your release, Cisco software supports BFD forwarding on point-to-point IPv4, IPv6, and generic routing encapsulation (GRE) tunnels.

Only numbered interfaces are allowed. When the tunnel type is changed from a supported tunnel type to an unsupported one, BFD sessions are brought down for that tunnel and the BFD configuration is removed from the interface.

BFD detection time depends on the topology and infrastructure. For a single-hop IP tunnel that is deployed across physically adjacent devices, the 150 ms (that is, a hello interval of 50 ms with up to three retries) detection rate applies. However, when the source and destination endpoints of the tunnel are not connected back-to-back, the 150 ms detection rate is not guaranteed.

BFD uses the IP address configured on the tunnel interface. It does not use the tunnel source and destination addresses.

BFD support on DMVPN

- NHRP currently acts only on BFD down events and not on up events.
- Both peers must configure BFD to get BFD support. If one of the peers is not configured with BFD, the other peer creates BFD sessions in down or unknown state.
- BFD intervals configured on the peers should be the same in the BFD echo mode for spoke to spoke refresh to work as expected.



Note NOTE - From Cisco IOS XE 17.11.1a, there is a new keyword delete for the ip nhrp bfd command. This keyword deletes the tunnel entry immediately on a BFD down event and changes the default behavior of deleting the tunnel entry after the expiry of the entry.

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.

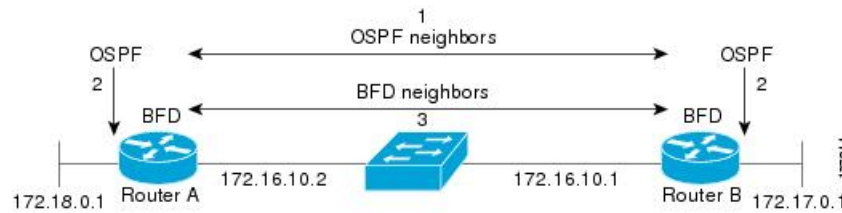


Note To enable BFD, it is recommended to use the BFD template configuration and enable the same BFD template under the interface, instead of directly configuring the BFD parameters under the interface.

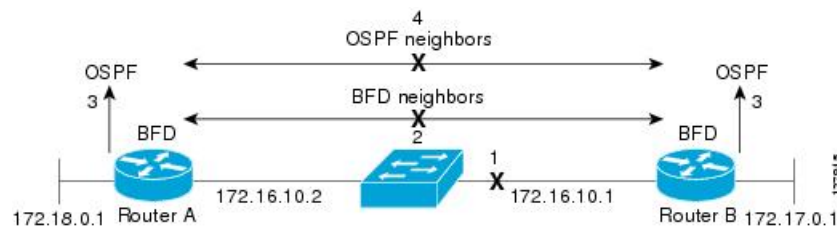
Neighbor Relationships

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.

BFD Detection of Failures

Once a BFD session has been established and timer negotiations are complete, BFD peers send BFD control packets that act in the same manner as an IGP hello protocol to detect liveness, 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.

BFD Version Interoperability

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.

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

BFD Support for Nonbroadcast Media Interfaces

The **bfd interval** command must be configured on the interface to initiate BFD monitoring.

BFD Support for VPN Routing and Forwarding Interfaces

The BFD feature is extended

to be VPN Routing and Forwarding (VRF) aware to provide fast detection of routing protocol failures between provider edge (PE) and customer edge (CE) routers.

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 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

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.

Multi-hop BFD over IPv6 is supported in software mode only.

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:

- 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.

Benefits of BFD Support on DMVPN

- Faster detection of link failure.
- In non-crypto deployments, spoke can detect hub failure only after NHRP registration timeout but hub cannot detect a spoke failure until cache on hub expires (even though routing can re-converge much earlier). BFD allows for a very fast detection for such a failure.
- BFD validates the forwarding path between non authoritative sessions, for example, in scenarios where the hub is configured to respond on behalf of the spoke.
- BFD validates end-to-end data path including the tunnel unlike IKE keepalives/DPD that doesn't pass through the tunnel.
- BFD probes can be off-loaded.

There is no special NHRP configuration needed for BFD support on DMVPN, enabling BFD on an NHRP enabled interface suffices. For DMVPN configuration, refer [How to Configure Dynamic Multipoint VPN](#).

How to Configure Bidirectional Forwarding Detection

Configuring BFD Session Parameters on the Interface

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Perform one of the following steps:
 - **ip address** *ipv4-address mask*
 - **ipv6 address** *ipv6-address/mask*
4. **end**

DETAILED STEPS

Procedure

Step 1

enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2

configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3

Perform one of the following steps:

- **ip address** *ipv4-address mask*
- **ipv6 address** *ipv6-address/mask*

Example:

Configuring an IPv4 address for the interface:

```
Device(config-if)# ip address 10.201.201.1 255.255.255.0
```

Configuring an IPv6 address for the interface:

```
Device(config-if)# ipv6 address 2001:db8:1:1::1/32
```

Configures an IP address for the interface.

Step 4

end

Example:

```
Device(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

Configuring BFD Support for Dynamic Routing Protocols

You can enable BFD support for dynamic routing protocols at the router level to enable BFD support globally for all interfaces or you can configure BFD on a per-interface basis at the interface level.

This section describes the following procedures:

Configuring BFD Support for BGP

This section describes the procedure for configuring BFD support for BGP so that BGP is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD.

Before you begin

BGP must be running on all participating routers.

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.



Note Output from the **show bfd neighbors details** command shows the configured intervals. The output does not show intervals that were changed because hardware-offloaded BFD sessions were configured with Tx and Rx intervals that are not multiples of 50 ms.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-tag*
4. **neighbor** *ip-address* **fall-over bfd**
5. **end**
6. **show bfd neighbors [details]**

7. show ip bgp neighbor

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	router bgp <i>as-tag</i> Example: <pre>Router(config)# router bgp tag1</pre>	Specifies a BGP process and enters router configuration mode.
Step 4	neighbor <i>ip-address</i> fall-over bfd Example: <pre>Router(config-router)# neighbor 172.16.10.2 fall-over bfd</pre>	Enables BFD support for fallover.
Step 5	end Example: <pre>Router(config-router)# end</pre>	Exits router configuration mode and returns the router to privileged EXEC mode.
Step 6	show bfd neighbors [details] Example: <pre>Router# show bfd neighbors detail</pre>	(Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. Note If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the show bfd neighbors details command will show the configured intervals, not the changed ones.
Step 7	show ip bgp neighbor Example: <pre>Router# show ip bgp neighbor</pre>	(Optional) Displays information about BGP and TCP connections to neighbors.

What to Do Next

See the Monitoring and Troubleshooting BFD section for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections.

Configuring BFD Support for EIGRP

This section describes the procedure for configuring BFD support for EIGRP so that EIGRP is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD. There are two methods for enabling BFD support for EIGRP:

- You can enable BFD for all of the interfaces for which EIGRP is routing by using the **bfd all-interfaces** command in router configuration mode.
- You can enable BFD for a subset of the interfaces for which EIGRP is routing by using the **bfd interface type number** command in router configuration mode.

Before you begin

EIGRP must be running on all participating routers.

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.



Note Output from the **show bfd neighbors details** command shows the configured intervals. The output does not show intervals that were changed because hardware-offloaded BFD sessions were configured with Tx and Rx intervals that are not multiples of 50 ms.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp as-number**
4. Do one of the following:
 - **bfd all-interfaces**
 - **bfd interface type number**
5. **end**
6. **show bfd neighbors [details]**
7. **show ip eigrp interfaces [type number] [as-number] [detail]**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router eigrp as-number Example: Router(config)# router eigrp 123	Configures the EIGRP routing process and enters router configuration mode.
Step 4	Do one of the following: <ul style="list-style-type: none"> bfd all-interfaces bfd interface type number Example: Router(config-router)# bfd all-interfaces Example: Router(config-router)# bfd interface FastEthernet 6/0	Enables BFD globally on all interfaces associated with the EIGRP routing process. or Enables BFD on a per-interface basis for one or more interfaces associated with the EIGRP routing process.
Step 5	end Example: Router(config-router) end	Exits router configuration mode and returns the router to privileged EXEC mode.
Step 6	show bfd neighbors [details] Example: Router# show bfd neighbors details	(Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. Note If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the show bfd neighbors details command will show the configured intervals, not the changed ones.
Step 7	show ip eigrp interfaces [type number] [as-number] [detail] Example: Router# show ip eigrp interfaces detail	(Optional) Displays the interfaces for which BFD support for EIGRP has been enabled.

What to Do Next

See the Monitoring and Troubleshooting BFD section for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections.

Configuring BFD Support for IS-IS

This section describes the procedures for configuring BFD support for IS-IS so that IS-IS is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD. There are two methods for enabling BFD support for IS-IS:

- You can enable BFD for all of the interfaces on which IS-IS is supporting IPv4 routing by using the **bfd all-interfaces** command in router configuration mode. You can then disable BFD for one or more of those interfaces using the **isis bfd disable** command in interface configuration mode.
- You can enable BFD for a subset of the interfaces for which IS-IS is routing by using the **isis bfd** command in interface configuration mode.

To configure BFD support for IS-IS, perform the steps in one of the following sections:

Prerequisites

IS-IS must be running on all participating routers.

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



Note Output from the **show bfd neighbors details** command shows the configured intervals. The output does not show intervals that were changed because hardware-offloaded BFD sessions were configured with Tx and Rx intervals that are not multiples of 50 ms.

Configuring BFD Support for IS-IS for All Interfaces

To configure BFD on all IS-IS interfaces that support IPv4 routing, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **bfd all-interfaces**
5. **exit**
6. **interface** *type number*
7. **ip router isis** [*tag*]
8. **isis bfd** [**disable**]
9. **end**
10. **show bfd neighbors** [**details**]
11. **show clns interface**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	router isis area-tag Example: <pre>Router(config)# router isis tag1</pre>	Specifies an IS-IS process and enters router configuration mode.
Step 4	bfd all-interfaces Example: <pre>Router(config-router)# bfd all-interfaces</pre>	Enables BFD globally on all interfaces associated with the IS-IS routing process.
Step 5	exit Example: <pre>Router(config-router)# exit</pre>	(Optional) Returns the router to global configuration mode.
Step 6	interface type number Example: <pre>Router(config)# interface fastethernet 6/0</pre>	(Optional) Enters interface configuration mode.
Step 7	ip router isis [tag] Example: <pre>Router(config-if)# ip router isis tag1</pre>	(Optional) Enables support for IPv4 routing on the interface.
Step 8	isis bfd [disable] Example: <pre>Router(config-if)# isis bfd</pre>	(Optional) Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. Note You should use the disable keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the bfd all-interfaces command in router configuration mode.

	Command or Action	Purpose
Step 9	end Example: <pre>Router(config-if)# end</pre>	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 10	show bfd neighbors [details] Example: <pre>Router# show bfd neighbors details</pre>	(Optional) Displays information that can be used to verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. Note If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the show bfd neighbors details command will show the configured intervals, not the changed ones.
Step 11	show clns interface Example: <pre>Router# show clns interface</pre>	(Optional) Displays information that can be used to verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

What to Do Next

See the Monitoring and Troubleshooting BFD section for more information on monitoring and troubleshooting BFD. If you want to configure only for a specific subset of interfaces, perform the tasks in the Configuring BFD Support for IS-IS for One or More Interfaces section.

Configuring BFD Support for IS-IS for One or More Interfaces

To configure BFD for only one or more IS-IS interfaces, perform the steps in this section.



Note Output from the **show bfd neighbors details** command shows the configured intervals. The output does not show intervals that were changed because hardware-offloaded BFD sessions were configured with Tx and Rx intervals that are not multiples of 50 ms.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip router isis** [*tag*]
5. **isis bfd** [disable]
6. **end**
7. **show bfd neighbors** [details]
8. **show clns interface**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: <pre>Router(config)# interface fastethernet 6/0</pre>	Enters interface configuration mode.
Step 4	ip router isis [<i>tag</i>] Example: <pre>Router(config-if)# ip router isis tag1</pre>	Enables support for IPv4 routing on the interface.
Step 5	isis bfd [disable] Example: <pre>Router(config-if)# isis bfd</pre>	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. Note You should use the disable keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the bfd all-interfaces command in router configuration mode.
Step 6	end Example: <pre>Router(config-if)# end</pre>	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 7	show bfd neighbors [details] Example: <pre>Router# show bfd neighbors details</pre>	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. Note If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the show bfd neighbors details command will show the configured intervals, not the changed ones.

	Command or Action	Purpose
Step 8	show clns interface Example: Router# show clns interface	(Optional) Displays information that can help verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

What to Do Next

See the Monitoring and Troubleshooting BFD section for more information on monitoring and maintaining BFD. If you want to configure BFD support for another routing protocol, see one of the following sections.

Configuring BFD Support for OSPF

This section describes the procedures for configuring BFD support for OSPF so that OSPF is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD. You can either configure BFD support for OSPF globally on all interfaces or configure it selectively on one or more interfaces.

There are two methods for enabling BFD support for OSPF:

- You can enable BFD for all of the interfaces for which OSPF is routing by using the **bfd all-interfaces** command in router configuration mode. You can disable BFD support on individual interfaces using the **ip ospf bfd [disable]** command in interface configuration mode.
- You can enable BFD for a subset of the interfaces for which OSPF is routing by using the **ip ospf bfd** command in interface configuration mode.

See the following sections for tasks for configuring BFD support for OSPF:

Configuring BFD Support for OSPF for All Interfaces

To configure BFD for all OSPF interfaces, perform the steps in this section.

If you do not want to configure BFD on all OSPF interfaces and would rather configure BFD support specifically for one or more interfaces, see the Configuring BFD Support for OSPF for One or More Interfaces section.

Before you begin

OSPF must be running on all participating routers.

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.



Note Output from the **show bfd neighbors details** command shows the configured intervals. The output does not show intervals that were changed because hardware-offloaded BFD sessions were configured with Tx and Rx intervals that are not multiples of 50 ms.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **router ospf** *process-id*
4. **bfd all-interfaces** [**strict-mode**]
5. **exit**
6. **interface** *type number*
7. **ip ospf bfd** [**disable**]
8. **end**
9. **show bfd neighbors** [**details**]
10. **show ip ospf**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: <pre>Router(config)# router ospf 4</pre>	Specifies an OSPF process and enters router configuration mode.
Step 4	bfd all-interfaces [strict-mode] Example: <pre>Router(config-router)# bfd all-interfaces</pre>	Enables BFD globally on all interfaces associated with the OSPF routing process. [strict-mode] - BFD session is established in the strict-mode. In the strict-mode, the OSPF session is not established till the BFD session is established.
Step 5	exit Example: <pre>Router(config-router)# exit</pre>	(Optional) Returns the router to global configuration mode. Enter this command only if you want to perform Step 7 to disable BFD for one or more interfaces.
Step 6	interface <i>type number</i> Example: <pre>Router(config)# interface fastethernet 6/0</pre>	(Optional) Enters interface configuration mode. Enter this command only if you want to perform Step 7 to disable BFD for one or more interfaces.

	Command or Action	Purpose
Step 7	ip ospf bfd [disable] Example: <pre>Router(config-if)# ip ospf bfd disable</pre>	(Optional) Disables BFD on a per-interface basis for one or more interfaces associated with the OSPF routing process. Note You should use the disable keyword only if you enabled BFD on all of the interfaces that OSPF is associated with using the bfd all-interfaces command in router configuration mode.
Step 8	end Example: <pre>Router(config-if)# end</pre>	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 9	show bfd neighbors [details] Example: <pre>Router# show bfd neighbors detail</pre>	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. Note If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the show bfd neighbors details command will show the configured intervals, not the changed ones.
Step 10	show ip ospf Example: <pre>Router# show ip ospf</pre>	(Optional) Displays information that can help verify if BFD for OSPF has been enabled. If BFD is enabled in strict-mode, the command output displays BFD is enabled in strict mode.

What to Do Next

See the Monitoring and Troubleshooting BFD section for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections.

Configuring BFD Support for OSPF for One or More Interfaces

To configure BFD on one or more OSPF interfaces, perform the steps in this section.

Before you begin

OSPF must be running on all participating routers.

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.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface** *type number*
4. **ip ospf bfd** [**disable**] [**strict-mode**]
5. **end**
6. **show bfd neighbors** [**details**]
7. **show ip ospf**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: <pre>Router(config)# interface fastethernet 6/0</pre>	Enters interface configuration mode.
Step 4	ip ospf bfd [disable] [strict-mode] Example: <pre>Router(config-if)# ip ospf bfd</pre>	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the OSPF routing process. Note You should use the disable keyword only if you enabled BFD on all of the interfaces that OSPF is associated with using the bfd all-interfaces command in router configuration mode. [strict-mode] - BFD session is established in the strict-mode. In the strict-mode, the OSPF session is not established till the BFD session is established.
Step 5	end Example: <pre>Router(config-if)# end</pre>	Exits interface configuration mode and returns the router to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show bfd neighbors [details] Example: <pre>Router# show bfd neighbors details</pre>	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. Note If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the show bfd neighbors details command will show the configured intervals, not the changed ones.
Step 7	show ip ospf Example: <pre>Router# show ip ospf</pre>	(Optional) Displays information that can help verify if BFD support for OSPF has been enabled. If BFD is enabled in strict-mode, the command output displays <code>BFD is enabled in strict mode</code> .

What to Do Next

See the Monitoring and Troubleshooting BFD section for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections.

Configuring BFD Support for HSRP

Perform this task to enable BFD support for Hot Standby Router Protocol (HSRP.) Repeat the steps in this procedure for each interface over which you want to run BFD sessions to HSRP peers.

HSRP supports BFD by default. If HSRP support for BFD has been manually disabled, you can reenabling it at the router level to enable BFD support globally for all interfaces or on a per-interface basis at the interface level.

Before you begin

- HSRP must be running on all participating routers.
- Cisco Express Forwarding must be enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]
7. **standby bfd**
8. **exit**
9. **standby bfd all-interfaces**
10. **exit**
11. **show standby neighbors**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	ip cef [distributed] Example: <pre>Router(config)# ip cef</pre>	Enables Cisco Express Forwarding or distributed Cisco Express Forwarding.
Step 4	interface <i>type number</i> Example: <pre>Router(config)# interface FastEthernet 6/0</pre>	Enters interface configuration mode.
Step 5	ip address <i>ip-address mask</i> Example: <pre>Router(config-if)# ip address 10.0.0.11 255.255.255.0</pre>	Configures an IP address for the interface.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [<i>secondary</i>]] Example: <pre>Router(config-if)# standby 1 ip 10.0.0.11</pre>	Activates HSRP.
Step 7	standby bfd Example: <pre>Router(config-if)# standby bfd</pre>	(Optional) Enables HSRP support for BFD on the interface.
Step 8	exit Example: <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.
Step 9	standby bfd all-interfaces Example:	(Optional) Enables HSRP support for BFD on all interfaces.

	Command or Action	Purpose
	<code>Router(config)# standby bfd all-interfaces</code>	
Step 10	exit Example: <code>Router(config)# exit</code>	Exits global configuration mode.
Step 11	show standby neighbors Example: <code>Router# show standby neighbors</code>	(Optional) Displays information about HSRP support for BFD.

What to Do Next

See the Monitoring and Troubleshooting BFD section for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections.

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

- enable**
- configure terminal**
- interface** *type number*
- Perform one of the following steps:
 - ip address** *ipv4-address mask*
 - ipv6 address** *ipv6-address/mask*
- exit**
- Perform one of the following steps:
 - ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]]
 - ipv6 route static bfd** *interface-type interface-number ip-address* [**unaasosiated**]
- Perform one of the following steps:
 - ip route** [**vrf** *vrf-name*] *prefix mask {ip-address | interface-type interface-number [ip-address]}* [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
 - ipv6 route** [**vrf** *vrf-name*] *ipv6 prefix/mask {ipv6-address | interface-type interface-number [ipv6-address]}* [**name** *next-hop-name*] [**track** *number*] [**tag** *tag*]
- exit**
- Perform one of the following steps:

- **show ip static route**
 - **show ipv6 static**
10. Perform one of the following steps:
- **show ip static route bfd**
 - **show ipv6 static bfd**
11. **exit**

DETAILED STEPS

Procedure

Step 1

enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2

configure terminal

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3

interface *type number*

Example:

```
Device(config)# interface
```

Configures an interface and enters interface configuration mode.

Step 4

Perform one of the following steps:

- **ip address *ipv4-address mask***
- **ipv6 address *ipv6-address/mask***

Example:

Configuring an IPv4 address for the interface:

```
Device(config-if)# ip address 10.201.201.1 255.255.255.0
```

Configuring an IPv6 address for the interface:

```
Device(config-if)# ipv6 address 2001:db8:1:1::1/32
```

Configures an IP address for the interface.

Step 5 **exit**

Example:

```
Device(config-if)# exit
```

Exits interface configuration mode and returns to global configuration mode.

Step 6 Perform one of the following steps:

- **ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]]
- **ipv6 route static bfd** *interface-type interface-number ip-address* [**unaasosiated**]

Example:

```
Device(config)# ip route static bfd 10.1.1.1 group group1 passive
```

```
Device(config)# ipv6 route static bfd TenGigabitEthernet 0/0/7 19:1:1::2
```

Specifies a static route BFD neighbor.

- The *interface-type*, *interface-number*, and *ip-address* arguments are required because BFD support exists only for directly connected neighbors.

Step 7 Perform one of the following steps:

- **ip route** [**vrf** *vrf-name*] *prefix mask {ip-address | interface-type interface-number [ip-address]}* [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
- **ipv6 route** [**vrf** *vrf-name*] *ipv6 prefix/mask {ipv6-address | interface-type interface-number [ipv6-address]}* [**name** *next-hop-name*] [**track** *number*] [**tag** *tag*]

Example:

```
Device(config)# ip route 10.0.0.0 255.0.0.0
```

```
Device(config)# ipv6 route 19:1:1::/64 TenGigabitEthernet0/0/7 19:1:1::2
```

Specifies a static route BFD neighbor.

Step 8 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Step 9 Perform one of the following steps:

- **show ip static route**
- **show ipv6 static**

Example:

(Optional) Displays static route database information.

Step 10 Perform one of the following steps:

- **show ip static route bfd**
- **show ipv6 static bfd**

Example:

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

Step 11 **exit****Example:**

```
Device# exit
```

Exits privileged EXEC mode and returns to user EXEC mode.

Configuring BFD Echo Mode

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

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

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

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 icmp 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

- BFD echo mode does not work in conjunction with Unicast Reverse Path Forwarding (uRPF) configuration. If both BFD echo mode and uRPF configurations are enabled, the sessions will flap.
- The use of echo mode for single hop BFD sessions on unnumbered interfaces is unreliable and may result in inability to properly detect failures. It is strongly recommended that echo mode be disabled when using single hop BFD on unnumbered interfaces.

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

Procedure

Step 1

enable

Example:

```
Switch> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2

configure terminal

Example:

```
Switch# configure terminal
```

Enters global configuration mode.

Step 3

bfd slow-timer *milliseconds*

Example:

```
Switch(config)# bfd slow-timer 12000
```

Configures the BFD slow timer.

Step 4

end

Example:

```
Switch(config)# end
```

Exits global configuration mode and returns the router to privileged EXEC mode.

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. **configure interface**
4. **no bfd echo**
5. **end**

DETAILED STEPS

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **configure interface**

Example:

```
Router(config)# configure interface
```

Enters interface configuration mode.

Step 4 **no bfd echo**

Example:

```
Router(config-if)# no bfd echo
```

Disables BFD echo mode.

- Use the **no** form to disable BFD echo mode.

Step 5 **end**

Example:

```
Router(config-if)# end
```

Exits global configuration mode and returns to privileged EXEC mode.

Creating and Configuring BFD Templates

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

Configuring a Single-Hop Template

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

Step 1

enable

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2

configure terminal

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3

bfd-template single-hop *template-name*

Example:

```
Router(config)# bfd-template single-hop bfdtemplate1
```

Creates a single-hop BFD template and enters BFD configuration mode.

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
```

Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.

Step 5 **end**

Example:

```
Router(bfd-config)# end
```

Exits BFD configuration mode and returns the router to privileged EXEC mode.

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

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **bfd-template multi-hop** *template-name*

Example:

```
Router(config)# bfd-template multi-hop mh-template1
```

Creates a BFD multihop BFD template and enters BFD configuration mode.

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
```

Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.

Step 5 **authentication** *authentication-type* **keychain** *keychain-name*

Example:

```
Router(bfd-config)# authentication keyed-sha-1 keychain bfd-multihop
```

Configures authentication for the multihop template and specifies the authentication type.

Step 6 **end**

Example:

```
Router(bfd-config)# end
```

Exits BFD configuration mode and returns the router to privileged EXEC mode.

Configuring BFD Support on DMVPN

BFD intervals can be directly configured on tunnel interface as shown below:

```
enable
configure terminal
interface tunnell
bfd interval 1000 min_rx 1000 multiplier 5
no echo
```

BFD intervals can also be configured by defining a template and attaching it to the tunnel interface as shown below

```
enable
configure terminal
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 5
interface tunnell
bfd template sample
```

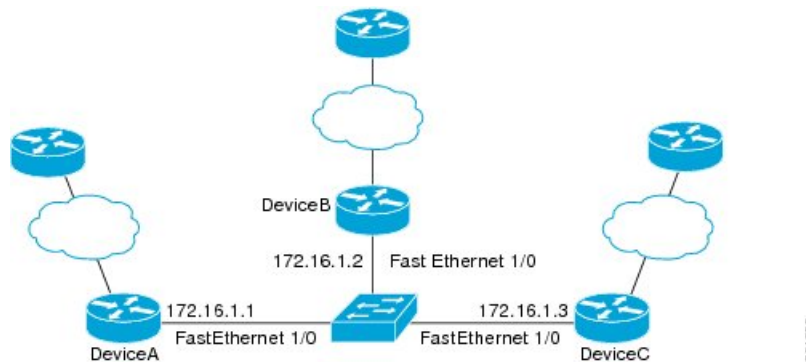
Configuration Examples for Bidirectional Forwarding Detection

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. Fast Ethernet interface 1/0 on RouterA is connected to the same network as Fast Ethernet interface 1/0 on Router B. Fast Ethernet interface 1/0 on RouterB is connected to the same network as Fast Ethernet interface 1/0 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 figure below shows a large EIGRP network with several routers, three of which are BFD neighbors that are running EIGRP as their routing protocol.



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

Configuration for RouterA

```
interface Fast Ethernet0/0
no shutdown
ip address 10.4.9.14 255.255.255.0
duplex auto
speed auto
!
interface Fast Ethernet1/0
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 Fast Ethernet0/0
  no shutdown
  ip address 10.4.9.34 255.255.255.0
  duplex auto
  speed auto
!
interface Fast Ethernet1/0
  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 Fast Ethernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface Fast Ethernet1/0
 ip address 172.16.1.3 255.255.255.0
 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    Fa1/0
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      Fa1/0
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**

```

OurAddr      NeighAddr
  LD/RD  RH/RS  Holdown(mult)  State    Int
172.16.1.2    172.16.1.1
  1/6    Up      0    (3 )    Up      Fa1/0
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

```

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

```

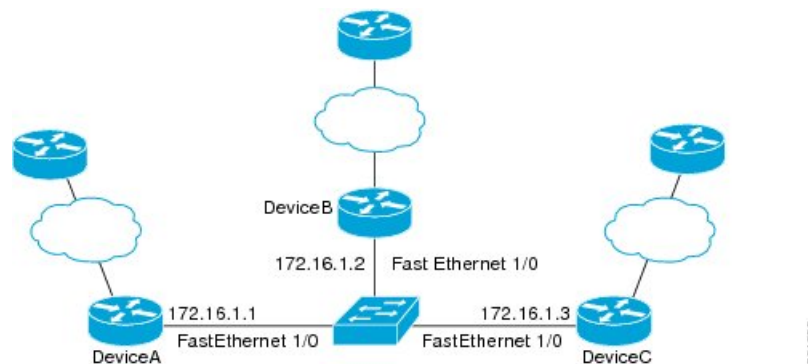
Last packet: Version: 1
- Diagnostic: 0
  State bit: Up          - Demand bit: 0
  Poll bit: 0           - Final bit: 0
  Multiplier: 3         - Length: 24
  My Discr.: 6          - Your Discr.: 1
  Min tx interval: 1000000 - Min rx interval: 1000000
  Min Echo interval: 50000

OurAddr      NeighAddr

  LD/RD  RH/RS  Holdown(mult)  State      Int
172.16.1.2  172.16.1.3
          3/6    1(RH)        118 (3 )    Up        Fal/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(5735)
Rx Count: 5731, Rx Interval (ms) min/max/avg: 32/72/49 last: 32 ms ago
Tx Count: 5740, Tx Interval (ms) min/max/avg: 40/64/50 last: 44 ms ago
Registered protocols: EIGRP
Uptime: 00:04:45
Last packet: Version: 0
- Diagnostic: 0
  I Hear You bit: 1      - Demand bit: 0
  Poll bit: 0           - Final bit: 0
  Multiplier: 3         - Length: 24
  My Discr.: 6          - Your Discr.: 3
  Min tx interval: 50000 - Min rx interval: 50000
  Min Echo interval: 0

```

The figure below shows that Fast Ethernet interface 1/0 on RouterB has failed. When Fast Ethernet interface 1/0 on RouterB is shut down, the BFD statistics of the corresponding BFD sessions on RouterA and RouterB are reduced.



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

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

```

RouterA# show bfd neighbors
OurAddr      NeighAddr

  LD/RD  RH/RS  Holdown(mult)  State      Int
172.16.1.1  172.16.1.3

```

```
5/3 1(RH) 134 (3 ) Up Fa1/0
```

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 Fa1/0
```

Example: Configuring BFD in an OSPF Network

In the following example, the simple OSPF network consists of Router A and Router B. Fast Ethernet interface 0/1 on Router A is connected to the same network as Fast Ethernet interface 6/0 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 Fast Ethernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
 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 Fast Ethernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
 ip address 172.18.0.1 255.255.255.0
!
router ospf 123
 log-adjacency-changes detail
 network 172.16.0.0 0.0.255.255 area 0
 network 172.18.0.0 0.0.255.255 area 0
 bfd all-interfaces
```

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

Router A

```
RouterA# show bfd neighbors details
OurAddr      NeighAddr    LD/RD RH  Holdown(mult)  State    Int
172.16.10.1  172.16.10.2  1/2  1    532 (3 )      Up       Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: OSPF
```

Uptime: 02:18:49

Last packet: Version: 0

```
- Diagnostic: 0
  I Hear You bit: 1    - Demand bit: 0
  Poll bit: 0          - Final bit: 0
  Multiplier: 3        - Length: 24
  My Discr.: 2         - Your Discr.: 1
  Min tx interval: 50000 - Min rx interval: 1000
  Min Echo interval: 0
```

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

Router B

```
RouterB# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
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       Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0          - Diagnostic: 0
                  I Hear You bit: 1    - Demand bit: 0
                  Poll bit: 0          - Final bit: 0
                  Multiplier: 5        - Length: 24
                  My Discr.: 1         - Your Discr.: 8
                  Min tx interval: 200000 - Min rx interval: 200000
                  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
```

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

Router A

RouterA# **show ip ospf**

```
Routing Process "ospf 123" with ID 172.16.10.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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
```

Example: Configuring BFD in an OSPF Network

```

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 Fast Ethernet 0/1
show ip ospf interface Fast Ethernet 0/1
Fast Ethernet0/1 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 Fast Ethernet 6/1
Fast Ethernet6/1 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. Fast Ethernet interface 0/1 on Router A is connected to the same network as Fast Ethernet interface 6/0 in Router B. The example, starting in global configuration mode, shows the configuration of BFD.

Configuration for Router A

```
!  
interface Fast Ethernet 0/1  
  ip address 172.16.10.1 255.255.255.0  
  bfd interval 50 min_rx 50 multiplier 3  
!  
interface Fast Ethernet 3/0.1  
  ip address 172.17.0.1 255.255.255.0  
!  
!  
router bgp 40000  
  bgp log-neighbor-changes  
  neighbor 172.16.10.2 remote-as 45000  
  neighbor 172.16.10.2 fall-over bfd  
  !  
  address-family ipv4  
  neighbor 172.16.10.2 activate  
  no auto-summary  
  no synchronization  
  network 172.18.0.0 mask 255.255.255.0  
  exit-address-family  
!
```

Configuration for Router B

```
!  
interface Fast Ethernet 6/0  
  ip address 172.16.10.2 255.255.255.0  
  bfd interval 50 min_rx 50 multiplier 3  
!  
interface Fast Ethernet 6/1  
  ip address 172.18.0.1 255.255.255.0  
!  
router bgp 45000  
  bgp log-neighbor-changes  
  neighbor 172.16.10.1 remote-as 40000  
  neighbor 172.16.10.1 fall-over bfd  
  !  
  address-family ipv4  
  neighbor 172.16.10.1 activate  
  no auto-summary  
  no synchronization  
  network 172.17.0.0 mask 255.255.255.0  
  exit-address-family  
!
```

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

Router A

```
RouterA# show bfd neighbors details
```

```
OurAddr      NeighAddr    LD/RD RH  Holdown(mult)  State    Int
172.16.10.1  172.16.10.2   1/8  1    332 (3 )      Up       Fa0/1
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 from the line card on Router B verifies that a BFD session has been created:

Router B

```
RouterB# attach 6
```

```
Entering Console for 8 Port Fast Ethernet in Slot: 6
```

```
Type "exit" to end this session
```

```
Press RETURN to get started!
```

```
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       Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0          - Diagnostic: 0
              I Hear You bit: 1   - Demand bit: 0
              Poll bit: 0         - Final bit: 0
              Multiplier: 5       - Length: 24
              My Discr.: 1        - Your Discr.: 8
              Min tx interval: 200000 - Min rx interval: 200000
              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
```

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 fallover
.
.
.
```

Router B

```
RouterB# show ip bgp neighbors
BGP neighbor is 172.16.10.1, remote AS 40000, external link
  Using BFD to detect fast fallover
.
.
.
```

Example: Configuring BFD in an IS-IS Network

In the following example, the simple IS-IS network consists of Router A and Router B. Fast Ethernet interface 0/1 on Router A is connected to the same network as Fast Ethernet interface 6/0 for Router B. The example, starting in global configuration mode, shows the configuration of BFD.

Configuration for Router A

```
!
interface Fast Ethernet 0/1
 ip address 172.16.10.1 255.255.255.0
 ip router isis
  bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
 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 Fast Ethernet 6/0
 ip address 172.16.10.2 255.255.255.0
 ip router isis
  bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
 ip address 172.18.0.1 255.255.255.0
 ip router isis
!
router isis
 net 49.0000.0000.0002.00
  bfd all-interfaces
!
```

Example: Configuring BFD in an IS-IS Network

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

```
RouterA# show bfd neighbors details
```

```
OurAddr      NeighAddr    LD/RD RH  Holdown(mult)  State    Int
172.16.10.1  172.16.10.2  1/8 1    536 (3 )      Up       Fa0/1
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:

```
RouterB# attach 6
```

```
Entering Console for 8 Port Fast Ethernet in Slot: 6
```

```
Type "exit" to end this session
```

```
Press RETURN to get started!
```

```
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       Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0          - Diagnostic: 0
              I Hear You bit: 1   - Demand bit: 0
              Poll bit: 0         - Final bit: 0
              Multiplier: 5       - Length: 24
              My Discr.: 1        - Your Discr.: 8
              Min tx interval: 200000 - Min rx interval: 200000
              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
```

Example: Configuring BFD in an HSRP Network

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



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

Router A

```
ip cef
interface Fast Ethernet2/0
  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 Fast Ethernet2/0
  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 Fast Ethernet2/0
  10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !
RouterB# show standby neighbors

HSRP neighbors on Fast Ethernet2/0
  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
ip route static bfd Serial 2/0 10.201.201.2
ip route 10.0.0.0 255.0.0.0 Serial 2/0 10.201.201.2
```

Device B

```
configure terminal
interface Serial 2/0
ip address 10.201.201.2 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.1
ip route 10.1.1.1 255.255.255.255 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 Ethernet interface 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 Ethernet 0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
```

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

```
configure terminal
ip route static bfd Ethernet 0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
ip route static bfd Ethernet 0/0.1001 209.165.200.226 group testgroup passive
ip route 10.1.1.1 255.255.255.224 Ethernet 0/0.1001 209.165.200.226
ip route 10.2.2.2 255.255.255.224 Ethernet 0/0.1001 209.165.200.226
```

Example: BFD Support on DMVPN

Example: BFD Support on DMVPN

The following is an example of configuring BFD support on DMVPN on hub.

```
bfd-template single-hop sample
  interval min-tx 1000 min-rx 1000 multiplier 5
!
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  no ip redirects
  ip nhrp authentication cisco123
  ip nhrp network-id 5
  ip nhrp redirect
  ip mtu 1400
  ip tcp adjust-mss 1360
  bfd template sample
  tunnel source GigabitEthernet0/0/0
  tunnel mode gre multipoint
  tunnel key 6
!
interface GigabitEthernet0/0/0
  ip address 10.0.0.1 255.0.0.0
  negotiation auto
!
router eigrp 2
network 10.0.0.0 0.0.0.255
bfd all-interfaces
auto-summary
!
```

The following is an example of configuring BFD support on DMVPN on spoke.

```
bfd-template single-hop sample
  interval min-tx 1000 min-rx 1000 multiplier 5
!
interface Tunnel1
  ip address 10.0.0.10 255.255.255.0
  no ip redirects
  ip nhrp authentication cisco123
  ip nhrp network-id 5
  ip nhrp nhs 10.0.0.1 nbma 10.0.0.10 multicast
  bfd template sample
  tunnel source GigabitEthernet0/0/0
  tunnel mode gre multipoint
  tunnel key 6
!
interface GigabitEthernet0/0/0
  mtu 4000
  ip address 11.0.0.1 255.0.0.0
  media-type rj45
  negotiation auto
!
interface GigabitEthernet0/0/1
  mtu 6000
  ip address 111.0.0.1 255.255.255.0
  negotiation auto
```

```

!
router eigrp 2
 network 11.0.0.0 0.0.0.255
 network 111.0.0.0 0.0.0.255
 network 10.0.0.0 0.0.0.255
bfd all-interfaces
auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2

```

The following example outlines how to delete the tunnel entry details when BFD support is down by addition of `ip nhrp bfd` command. By default, the tunnel entry is not immediately deleted and is deleted after expiry of the entry.

```

!
interface Tunnel0
ip address 10.0.1.100 255.255.255.0
no ip redirects
ip nhrp authentication testing
ip nhrp summary-map 192.168.0.0/16 72.68.100.2
ip nhrp summary-map 77.77.0.0/16 72.68.100.2
ip nhrp network-id 100
ip nhrp bfd delete
ip nhrp redirect
bfd interval 1000 min_rx 1000 multiplier 5
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 100
tunnel protection ipsec profile default
!

```



Note In this configuration, the tunnel entry is immediately deleted upon receiving a BFD down event. Without this configuration, the cache entry pertaining to the tunnel address of the peer is not deleted and performs its default behaviour.

The following is an example to illustrate faster convergence on spoke.

```

interface Tunnell
ip address 18.0.0.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp network-id 12
ip nhrp nhs 10.0.0.1 nbma 10.0.0.10 multicast
bfd template sample
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel key 18
tunnel protection ipsec profile MY_PROFILE
!
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 3
echo
!
router eigrp 2
bfd interface Tunnell -----> Specify the interface on which the routing
 protocol must act for BFD up/down events
 network 11.0.0.0 0.0.0.255

```



```
network 111.0.0.0 0.0.0.255
```

With the above configuration, as soon as BFD is reported down (3 seconds to detect), EIGRP will remove the routes installed from RIB.

The following sample output shows a summary output on hub:

```
device#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
=====

Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
-----
      1 172.17.0.1          10.0.0.1   UP 00:00:14      D
      1 172.17.0.2          10.0.0.2   BFD 00:00:03      D
```

BFD is a new state which implies that while the session is UP as seen by lower layers (IKE, IPSec and NHRP), BFD sees the session as DOWN. As usual, the state is an indication of the lower most layer where the session is not UP. Also, this applies only to the parent cache entry. This could be because it was detected as DOWN by BFD or BFD is not configured on the other side.

The following sample output shows a summary output on spoke:

```
device#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
=====

Interface: Tunnel2, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
-----
      2 172.17.0.2          10.0.0.2   BFD 00:00:02      DT1
      10.0.0.2          10.0.0.2   UP 00:00:02      DT2
      1 172.17.0.11         10.0.0.11   UP 00:05:35      S
```

The following sample shows output for **show ip/ipv6 nhrp** command

```
device#show ip nhrp
10.0.0.2/32 via 10.0.0.2
    Tunnel2 created 00:00:15, expire 00:04:54
```

```

Type: dynamic, Flags: router nhop rib bfd
NBMA address: 172.17.0.2
10.0.0.11/32 via 10.0.0.11
Tunnel2 created 00:09:04, never expire
Type: static, Flags: used bfd
NBMA address: 172.17.0.11
192.168.1.0/24 via 10.0.0.1
Tunnel2 created 00:00:05, expire 00:04:54
Type: dynamic, Flags: router unique local
NBMA address: 172.17.0.1
(no-socket)
192.168.2.0/24 via 10.0.0.2
Tunnel2 created 00:00:05, expire 00:04:54
Type: dynamic, Flags: router rib nho
NBMA address: 172.17.0.2

```

BFD flag here implies that there is a BFD session for this peer. This marking is only for parent entries.

The following sample shows output for **show tunnel endpoints** command

```

device#show tunnel endpoints
Tunnel2 running in multi-GRE/IP mode

Endpoint transport 172.17.0.2 Refcount 3 Base 0x2ABF53ED09F0 Create Time 00:00:07
overlay 10.0.0.2 Refcount 2 Parent 0x2ABF53ED09F0 Create Time 00:00:07
Tunnel Subblocks:
  tunnel-nhrp-sb:
    NHRP subblock has 2 entries; BFD(0x2):U
Endpoint transport 172.17.0.11 Refcount 3 Base 0x2ABF53ED0B80 Create Time 00:09:07
overlay 10.0.0.11 Refcount 2 Parent 0x2ABF53ED0B80 Create Time 00:09:07
Tunnel Subblocks:
  tunnel-nhrp-sb:
    NHRP subblock has 1 entries; BFD(0x1):U

```

For every tunnel endpoint, a new text "**BFD(handle):state**" is added. State here is UP(U), DOWN(D), NONE(N) or INVALID(I).

- In case, BFD is not configured on peer or a session is not UP for the first time, then the state will be N.

The following sample shows output for **show nhrp interfaces** command. This shows the configuration (and not operational) states on the interface or globally.

```

device#show nhrp interfaces
NHRP Config State
-----
Global:
  BFD: Registered

Tunnel1:
  BFD: Disabled

Tunnel2:
  BFD: Enabled

```

This is an internal and hidden command. This will currently display if NHRP is client of BFD and if BFD is enabled on the NHRP interface.

Example: Disabling Echo Mode When Configuring Single-Hop BFD on Unnumbered Interfaces

BFD is configured on the interface using the `bfd interval` command

If BFD is configured on the interface using the `bfd interval` command, BFD echo is enabled by default; this is not recommended. To disable BFD echo, configure the `no bfd echo` command under the interface.

```
interface Ethernet0/0
ip unnumbered Loopback0 poll point-to-point
ip router isis 1
bfd interval 50 min_rx 50 multiplier 3
no bfd echo
isis network point-to-point
isis bfd
end
```

BFD is configured using the BFD template configuration

If BFD is configured using the BFD template configuration, then BFD echo is disabled by default. It is recommended that BFD echo is **not** enabled under the BFD template.

```
bfd-template single-hop max

interval min-tx 50 min-rx 50 multiplier 3
!
interface Ethernet0/0
ip unnumbered Loopback0 poll point-to-point
bfd template max
!
device(config)#bfd-template single-hop max
device(config-bfd)#?
  BFD template configuration commands:
    authentication  Authentication type
    dampening       Enable session dampening
    default         Set a command to its defaults
    echo            Use echo adjunct as bfd detection mechanism.
    exit            Exit from BFD template configuration mode
    interval        Transmit interval between BFD packets
    no              Negate a command or set its defaults

device(config-bfd)#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
Configuring and monitoring BGP	“Cisco BGP Overview” module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>

Related Topic	Document Title
Configuring and monitoring EIGRP	“Configuring EIGRP” module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
Configuring and monitoring HSRP	“Configuring HSRP” module of the <i>Cisco IOS IP Application Services Configuration Guide</i>
Configuring and monitoring IS-IS	“Configuring Integrated IS-IS” module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
Configuring and monitoring OSPF	“Configuring OSPF” module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
BFD commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i>
BGP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i>
EIGRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i>
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Application Services Command Reference</i>
IS-IS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i>
OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i>
BFD IPv6 Encapsulation Support	“BFD IPv6 Encapsulation Support” module
OSPFv3 for BFD	“OSPFv3 for BFD” module
Static Route Support for BFD over IPv6	“Static Route Support for BFD over IPv6” module

Standards and RFCs

Standard/RFC	Title
IETF Draft	<i>Bidirectional Forwarding Detection</i> , February 2009 (http://tools.ietf.org/html/draft-ietf-bfd-base-09)
IETF Draft	<i>BFD for IPv4 and IPv6 (Single Hop)</i> , February 2009 (http://tools.ietf.org/html/draft-ietf-bfd-v4v6-1hop-09)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Bidirectional Forwarding Detection

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 1: Feature Information for Bidirectional Forwarding Detection

Feature Name	Releases	Feature Information
BFD Echo Mode	12.2(33)SRB 12.4(9)T 15.0(1)S	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. And since 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.
BFD IPv6 Encapsulation Support	Cisco IOS XE Release 3.11S	This feature extends IPv6 support for BFD. The following command was introduced or modified: bfd interval
BFD Multihop	15.1(3)S 15.4(1)S	This feature supports multihop BFD for IPv4 and IPv6 addresses. The following commands were introduced or modified: authentication, bfd map, bfd-template, interval, show bfd neighbors, show bfd neighbor drops.

Feature Name	Releases	Feature Information
BFD—Static Route Support	12.2(33)SRC 15.0(1)M 15.0(1)S 15.0(1)SY 15.1(2)S 15.1(1)SG 15.4(1)S	<p>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 RIB.</p> <p>A single BFD session can be used by an IPv4 static client to track the reachability of next hops through a specific interface. A BFD group can be assigned for a set of BFD-tracked static routes.</p> <p>The following commands were introduced or modified: ip route static bfd and show ip static route bfd.</p>
BFD Support for IP Tunnel (GRE, with IP address)	15.1(1)SY	<p>This feature supports BFD forwarding on point-to-point IPv4, IPv6, and GRE tunnels.</p> <p>The following commands were introduced or modified: bfd.</p>
BFD Support over Port Channel	15.1(1)SY 15.1(2)SY	<p>This feature supports configuring BFD timers on port channel interface.</p> <p>The following commands were introduced or modified: bfd.</p>
BFD—VRF Support	12.2(33)SRC 15.0(1)M 15.0(1)S 15.1(1)SY	<p>The BFD feature support is extended to be VPN Routing and Forwarding (VRF) aware to provide fast detection of routing protocol failures between provider edge (PE) and customer edge (CE) devices.</p>
BFD—WAN Interface Support	12.2(33)SRC 15.0(1)M 15.0(1)S	<p>The BFD feature is supported on nonbroadcast media interfaces including ATM, POS, serial, and VLAN interfaces. BFD support also extends to ATM, FR, POS, and serial subinterfaces.</p> <p>The bfd interval command must be configured on the interface to initiate BFD monitoring.</p>

Feature Name	Releases	Feature Information
Bidirectional Forwarding Detection (standard implementation, Version 1)	12.0(31)S 12.0(32)S 12.2(33)SRB 12.2(33)SRC 12.2(18)SXE 12.2(33)SXH 12.4(9)T 12.4(11)T 12.4(15)T 15.0(1)S 15.4(1)S	This document describes how to enable the Bidirectional Forwarding Detection (BFD) protocol. 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. 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.
HSRP Support for BFD	12.2(33)SRC 12.4(11)T 12.4(15)T	In Release 12.4(11)T, support for HSRP was added. In Release 12.2(33)SRC, the number of BFD sessions that can be created has been increased, BFD support has been extended to ATM, FR, POS, and serial subinterfaces, the BFD feature has been extended to be VRF-aware, BFD sessions are placed in an “Admin Down” state during a planned switchover, and BFD support has been extended to static routing.
IS-IS Support for BFD over IPv4	12.0(31)S 12.2(18)SXE 12.2(33)SRA 12.4(4)T 15.0(1)S 15.4(1)S	BFD support for OSPF can be configured globally on all interfaces or configured selectively on one or more interfaces. When BFD support is configured with IS-IS as a registered protocol with BFD, IS-IS receives forwarding path detection failure messages from BFD.
OSPF Support for BFD over IPv4	12.0(31)S 12.2(18)SXE 12.2(33)SRA 12.4(4)T 15.0(1)S 15.1(1)SG	BFD support for OSPF can be configured globally on all interfaces or configured selectively on one or more interfaces. When BFD support is configured with OSPF as a registered protocol with BFD, OSPF receives forwarding path detection failure messages from BFD.

Feature Name	Releases	Feature Information
SSO—BFD	12.2(33)SRE 12.2(33)SXI2 12.2(33)XNE 15.0(1)S 15.1(1)SG	Network deployments that use dual RP routers and switches have a graceful restart mechanism to protect forwarding states across a switchover. This feature enables BFD to maintain sessions in a up state across switchovers.
SSO—BFD (Admin Down)	12.2(33)SRC 15.0(1)S	To support SSO, BFD sessions are placed in an “Admin Down” state during a planned switchover. The BFD configuration is synched from the active to standby processor, and all BFD clients re-register with the BFD process on the standby processor.
sVTI Support on BFD	Cisco IOS-XE 17.6.4 Cisco IOS-XE 17.9.1a	sVTI support on BFD is introduced in Cisco IOS-XE 17.6.4 release. This feature is also supported in Cisco IOS-XE 17.9.1a release.