Bidirectional Forwarding Detection

Last Updated: May 04, 2011

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. 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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 XE 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 XE software.

Restrictions for Bidirectional Forwarding Detection

- The Cisco implementation of BFD supports the following routing protocols: BGP, EIGRP, IS-IS, and OSPF.
- BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away. Multihop configurations are not supported.

# Information About Bidirectional Forwarding Detection

BFD Operation

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Cisco supports the 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, you must configure BFD on both systems (or BFD peers). Once BFD has been enabled on the interfaces and at the router level for the appropriate routing protocols, 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.

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).
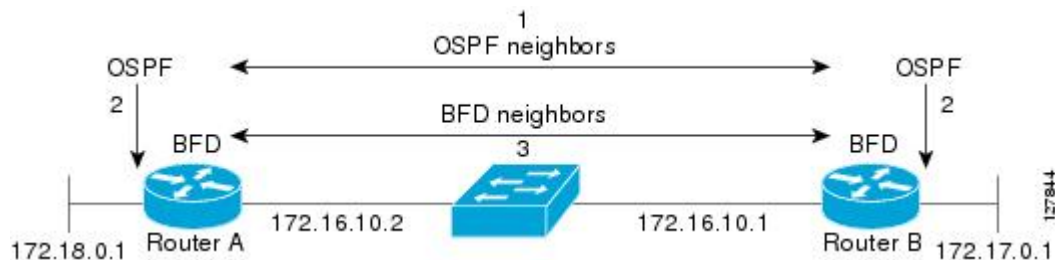
The figure below shows what happens when a failure occurs in the network (1). The BFD neighbor session with the OSPF neighbor router is torn down (2). BFD notifies the local OSPF process that the BFD neighbor is no longer reachable (3). The local OSPF process tears down the OSPF neighbor relationship (4). If an alternative path is available the routers will immediately start converging on it.
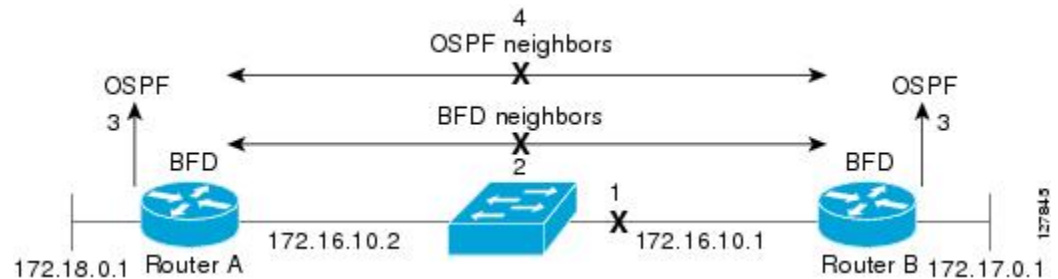
BFD Detection of Failures

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

- BFD is a forwarding path failure detection protocol. BFD detects a failure, but the routing protocol must take action to bypass a failed peer.
- Typically, BFD can be used at any protocol layer. For Cisco IOS XE Release 2.1, BFD is supported for static routing.

BFD Version Interoperability

All BFD sessions appear as Version 1 by default and are 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, of 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.

BFD Session

The maximum number of BFD sessions that can be created is 500. The maximum number of BFD sessions for a stateful switchover is 128.

BFD Support for Non-Broadcast Media Interfaces

The BFD feature is supported on non-broadcast media interfaces including ATM, POS, serial, and VLAN interfaces. BFD support extends to ATM, FR, POS, and serial subinterfaces as well.

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 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

Cisco IOS XE software supports BFD stateful switchover (SSO) for both planned and unplanned switchovers. 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 router 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 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 while 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 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 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.

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.

How to Configure Bidirectional Forwarding Detection

Configuring BFD Session Parameters on the Interface

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 6/0/0`	Enters interface configuration mode.
Step 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** `Router(config-if)# bfd interval 50 min_rx 50 multiplier 5`	Enables BFD on the interface.
Step 5	**end** **Example:** `Router(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.

For Cisco IOS XE Release 2.1, the Cisco implementation of BFD supports the following routing protocols: BGP, EIGRP, IS-IS, and OSPF.

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.

BGP must be running on all participating routers.

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

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

	Command or Action	Purpose
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	**router bgp** *as-tag* **Example:** Router(config)# router bgp tag1	Specifies a BGP process and enters router configuration mode.
Step 4	**neighbor** *ip-address* **fall-over bfd** **Example:** Router(config-router)# neighbor 172.16.10.2 fall-over bfd	Enables BFD support for fallover.
Step 5	**end** **Example:** Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] **Example:** Router# show bfd neighbors detail	(Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered.
Step 7	**show ip bgp neighbor**	(Optional) Displays information about BGP and TCP connections to neighbors.

Command or Action	Purpose
Example: `Router# show ip bgp neighbor`	

What to Do Next

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** command in router configuration mode.

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.

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

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. - Enter your password if prompted.

	Command or Action	Purpose
	Example: `Router> enable`	
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:
	
	• **bfd all-interfaces**
	•
	• **bfd interface** *type number*
	
	Example:
	
	`Router(config-router)# bfd all-interfaces`
	
	Example:
	
	Example:
	
	`Router(config-router)# bfd interface GigabitEthernet 6/0/0`
		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 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.
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

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.

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

	Command or Action	Purpose
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	**router isis** *area-tag* **Example:** Router(config)# router isis tag1	Specifies an IS-IS process and enters router configuration mode.
Step 4	**bfd all-interfaces** **Example:** Router(config-router)# bfd all-interfaces	Enables BFD globally on all interfaces associated with the IS-IS routing process.
Step 5	**exit** **Example:** Router(config-router)# exit	(Optional) Returns to global configuration mode.
Step 6	**interface** *type number* **Example:** Router(config)# interface gigabitethernet 6/0/0	(Optional) Enters interface configuration mode.
Step 7	**ip router isis** *[tag]* **Example:** Router(config-if)# ip router isis tag1	(Optional) Enables support for IPv4 routing on the interface.
Step 8	**isis bfd** [**disable**] **Example:** Router(config-if)# isis bfd	(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.
Step 9	**end**	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router(config-if)# end`	
Step 10	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	(Optional) Displays information that can be used to verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.
Step 11	**show clns interface** **Example:** `Router# show clns interface`	(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

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.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.

Command or Action	Purpose
Example: `Router# configure terminal`	
Step 3 **interface** *type number* **Example:** `Router(config)# interface gigabitethernet 6/0/0`	Enters interface configuration mode.
Step 4 **ip router isis** *[tag]* **Example:** `Router(config-if)# ip router isis tag1`	Enables support for IPv4 routing on the interface.
Step 5 **isis bfd [disable]** **Example:** `Router(config-if)# isis bfd`	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:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7 **show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.
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

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.

Prerequisites

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
	Example: Router# configure terminal	
Step 3	**router ospf** *process-id* **Example:** Router(config)# router ospf 4	Specifies an OSPF process and enters router configuration mode.
Step 4	**bfd all-interfaces** **Example:** Router(config-router)# bfd all-interfaces	Enables BFD globally on all interfaces associated with the OSPF routing process.
Step 5	**exit** **Example:** Router(config-router)# exit	(Optional) Returns 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** *type number* **Example:** Router(config)# interface gigabitethernet 6/0/0	(Optional) Enters interface configuration mode. Enter this command only if you want to perform Step 7 to disable BFD for one or more interfaces.
Step 7	**ip ospf bfd** [**disable**] **Example:** Router(config-if)# ip ospf bfd disable	(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:** Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 9	**show bfd neighbors** [**details**] **Example:** Router# show bfd neighbors detail	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.
Step 10	**show ip ospf** **Example:** Router# show ip ospf	(Optional) Displays information that can help verify if BFD for OSPF has been enabled.

What to Do Next

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.

Prerequisites

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, page 5 for more information.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
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	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 6/0/0`	Enters interface configuration mode.
Step 4	**ip ospf bfd** [**disable**] **Example:** `Router(config-if)# ip ospf bfd`	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.
Step 5	**end**	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router(config-if)# end`	
Step 6	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.
Step 7	**show ip ospf** **Example:** `Router# show ip ospf`	(Optional) Displays information that can help verify if BFD support for OSPF has been enabled.

What to Do Next

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
6. **ip route static bfd** *interface-type interface-number gateway*
7. **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*]
8. **end**
9. **show ip static route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface serial 2/0/0	Configures an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** Router(config-if)# ip address 10.201.201.1 255.255.255.0	Configures an IP address for the interface.
Step 5	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** Router(config-if)# bfd interval 500 min_rx 500 multiplier 5	Enables BFD on the interface.
Step 6	**ip route static bfd** *interface-type interface-number gateway* **Example:** Router(config-if)# ip route static bfd Serial 2/0/0 10.201.201.2	Specifies a static route BFD neighbor. • The *interface-type interface-number* and *gateway* arguments are required because BFD support exists only for directly connected neighbors.
Step 7	**ip route [vrf** *vrf-name* **]** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*] **Example:** Router(config-if)# ip route 10.0.0.0 255.0.0.0 **Example:** Serial 2/0/0 10.201.201.2	Specifies a static route BFD neighbor.
Step 8	**end** **Example:** Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 9	**show ip static route**	(Optional) Displays the static process local Routing Information Base (RIB) information.

Command or Action	Purpose
Example: `Router# show ip static route`	

Configuring BFD Echo Mode

This section contains the following configuration tasks for 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. 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.

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 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.

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

	Command or Action	Purpose
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 slow-timer** *milliseconds* **Example:** Router(config)# bfd slow-timer 12000	Configures the BFD slow timer.
Step 4	**end** **Example:** Router(config)# end	Exits global configuration mode and returns 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. **interface** *type number*
4. **no bfd echo**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface GigabitEthernet 6/0/0	Enters interface configuration mode.
Step 4	**no bfd echo** **Example:** Router(config-if)# no bfd echo	Disables BFD echo mode.
Step 5	**end** **Example:** Router(config-if)# end	Exits interface configuration mode and returns to global configuration mode.

Configuration Examples for Bidirectional Forwarding Detection

- Example Configuring BFD Support for Static Routing, page 21

Example Configuring BFD Support for Static Routing

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

Router A

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

Router B

```
configure terminal
  ip route static bfd Serial 2/0/0 10.201.201.1
  ip route 10.1.1.1 255.255.255.255 Serial 2/0/0 10.201.201.1
```

```
interface Serial 2/0/0
 ip address 10.201.201.2 255.255.255.0
 bfd interval 500 min_rx 500 multiplier 5
```

Note that the static route on Router 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.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
• Static route support for BFD in IPv6 • OSPF for IPv6 in BFD	" Implementing Bidirectional Forwarding Detection for IPv6 " module of the *Cisco IOS XE IPv6 Configuration Guide* , Release 2
Configuring and monitoring BGP	"Cisco BGP Overview" module of the *Cisco IOS XE IP Routing Protocols Configuration Guide* , Release 2
Configuring and monitoring EIGRP	"Configuring EIGRP" module of the *Cisco IOS XE IP Routing Protocols Configuration Guide* , Release 2
Configuring and monitoring IS-IS	"Integrated IS-IS Routing Protocol Overview "module of the *Cisco IOS XE IP Routing Protocols Configuration Guide* , Release 2
Configuring and monitoring OSPF	"Configuring OSPF " module of the *Cisco IOS XE IP Routing Protocols Configuration Guide* , Release 2
BFD commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: Protocol-Independent Command Reference*
BGP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: BGP Command Reference*
EIGRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: EIGRP Command Reference*
IS-IS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*

Related Topic	Document Title
OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: OSPF Command Reference*

Standards

Standard	Title
IETF Draft	*Bidirectional Forwarding Detection* , January 2006 (http://www.ietf.org/internet-drafts/draft-ietf-bfd-base-03.txt)
IETF Draft	*BFD for IPv4 and IPv6 (Single Hop)* , March 2005 (http://www.ietf.org/internet-drafts/draft-ietf-bfd-v4v6-1hop-02.txt)

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services	http://www.cisco.com/cisco/web/support/index.html

Description	Link
Newsletter, and Really Simple Syndication (RSS) Feeds.	
Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	

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
Bidirectional Forwarding Detection (standard implementation, Version 1)	Cisco IOS XE Release 2.1	This document describes how to enable the 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. 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. This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
BFD Echo Mode	Cisco IOS XE Release 2.1	BFD echo mode works with asynchronous BFD. Echo packets

Feature Name	Releases	Feature Information
		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.
		This feature was introduced on the Cisco ASR 1000 Series Routers.
BFD--EIGRP Support	Cisco IOS XE Release 2.1	BFD support for EIGRP can be configured so that EIGRP is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD.
		This feature was introduced on the Cisco ASR 1000 Series Routers.
BFD--VRF Support	Cisco IOS XE Release 2.1	The BFD feature support is extended to be VRF aware to provide fast detection of routing protocol failures between PE and CE routers.
		This feature was introduced on the Cisco ASR 1000 Series Routers.
BFD--WAN Interface Support	Cisco IOS XE Release 2.1	BFD feature is supported on non-broadcast media interfaces including ATM, POS, serial, and

Feature Name	Releases	Feature Information
		VLAN interfaces. BFD support extends to ATM, FR, POS, and serial subinterfaces as well.
		The **bfd interval** command must be configured on the interface to initiate BFD monitoring.
		This feature was introduced on the Cisco ASR 1000 Series Routers.
IS-IS Support for BFD over IPv4	Cisco IOS XE Release 2.1	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.
		This feature was introduced on the Cisco ASR 1000 Series Routers.
OSPF Support for BFD over IPv4	Cisco IOS XE Release 2.1	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.
		This feature was introduced on the Cisco ASR 1000 Series Routers.
SSO--BFD	Cisco IOS XE Release 2.1	This feature was introduced on the Cisco ASR 1000 Series Routers.
Static Routes for BFD	Cisco IOS XE Release 2.1	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

Feature Name	Releases	Feature Information
		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.
		This feature was introduced on the Cisco ASR 1000 Series Routers.