CHAPTER 39

Configuring Bidirectional Forwarding Detection

Note Starting with Cisco IOS Release IOS 15.1(1)SG, Bidirectional Forwarding Detection (BFD) support was introduced on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F Ethernet switches. With Cisco IOS XE 3.5.0E and IOS 15.2(1)E, supported was extended to Supervisor Engine 7-E, and Supervisor Engine 7L-E. With Cisco IOS XE 3.6.0E and IOS 15.2(2)E, supported was extended to Supervisor Engine 8-E.

This document describes how to enable the BFD protocol, which is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols.

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 are simplified, and reconvergence time is more consistent and predictable.

For details on all the BFD commands introduced in this chapter, see the URL:

http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_book.html

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 "Technical Assistance" section on page 39-29.

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

Contents

Prerequisites for Bidirectional Forwarding Detection

Prerequisites include:

- IP routing must be enabled on all participating switches.
- One of the IP routing protocols supported by BFD must be configured on the switches before BFD is deployed. You should implement fast convergence for the routing protocol that you plan to use. 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 on page 39-2 for more information on BFD routing protocol support in Cisco IOS software.

Restrictions for Bidirectional Forwarding Detection

Restrictions include:

- BFD Hardware offloading of sessions is not supported with the use of authentication on the 4500 Sup7E and Sup8E. Enable BFD Echo mode to work with authentication.
- BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away. Multihop configurations are not supported.

Cisco IOS Release 15.1(1)SG

- Cisco Catalyst 4500 series switches support up to 128 BFD sessions with a minimum hello interval of 50 ms and a multiplier of 3. The multiplier specifies the minimum number of consecutive packets that can be missed before a session is declared down.
- If SSO is enabled on a dual RP system, the following limitations apply:
  - The minimum hello interval is 50 ms with a multiplier of 5 or higher.
  - Smaller values may be configured but may flap during an SSO switchover.
- To enable echo mode the peer system must be configured with the **no ip redirects** command.

Cisco IOS Release XE 3.5.0E and IOS 15.2(1)E

- Cisco Catalyst 4500 series switches support up to 100 BFD sessions with a minimum hello interval of 100 ms and a multiplier of 3. The multiplier specifies the minimum number of consecutive packets that can be missed before a session is declared down.
- If SSO is enabled on a dual RP system, the following limitations apply:
  - The minimum hello interval is 50 ms with a multiplier of 5 or higher.
  - Smaller values may be configured but may flap during an SSO switchover.
- To enable echo mode the peer system must be configured with the **no ip redirects** command.

Note For the most accurate platform and hardware restrictions, see the Cisco IOS software release notes for your software version.

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 switches, 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 switches. Therefore, to create a BFD session, 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.

Cisco supports BFD echo mode. Echo packets are sent by the forwarding engine and are forwarded back along the same path to perform detection. The BFD session at the other end does not participate in the actual forwarding of the echo packets. See Configuring BFD Echo Mode, page 39-15 for more information.

This section includes the following subsections:

Neighbor Relationships

BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols BGP, EIGRP, OSPF, and static routes. By sending rapid failure detection notices to the routing protocols in the local switch to initiate the routing table recalculation process, BFD contributes to greatly reduced overall network convergence time. Figure 39-1 shows a simple network with two switches 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 routers (2). The BFD neighbor session with the OSPF neighbor router is established (3).

Figure 39-1 Establishing a BFD Neighbor Relationship

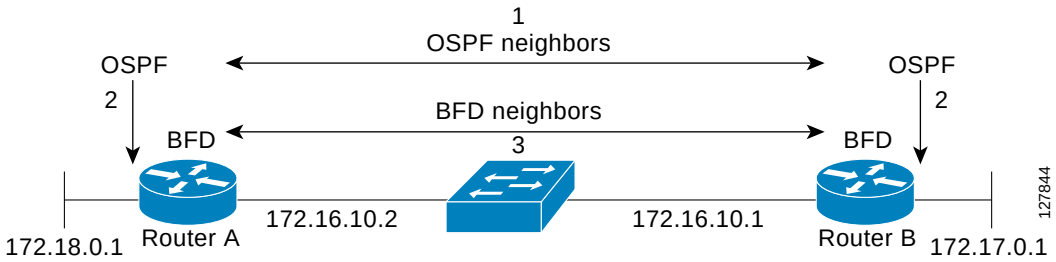
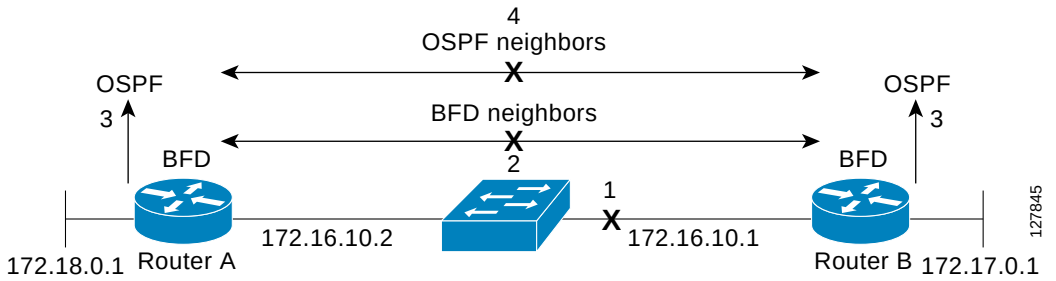


Figure 39-2 shows what happens when a failure occurs in the network (1). The BFD neighbor session with the OSPF neighbor router is torn down (2). BFD notifies the local OSPF process that the BFD neighbor is no longer reachable (3). The local OSPF process tears down the OSPF neighbor relationship (4). If an alternative path is available, the routers will immediately start converging on it.

Figure 39-2 Tearing Down an OSPF Neighbor Relationship



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 switches (routers) in DROTHER state.

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. However, the Cisco implementation of BFD supports only Layer 3 clients, in particular, the BGP, EIGRP, and OSPF routing protocols, and static routing.

- Cisco devices will use one BFD session for multiple client protocols in the Cisco implementation of BFD. For example, if a network is running OSPF and EIGRP across the same link to the same peer, only one BFD session will be established, and BFD will share session information with both routing protocols. However, IPv4 and IPv6 clients cannot share a BFD session.

BFD Version Interoperability

Starting with Cisco IOS Release 15.1(1)SG, the Catalyst 4500 series switch supports BFD Version 1 as well as BFD Version 0. All BFD sessions come up as Version 1 by default and will be interoperable with Version 0. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, if one BFD neighbor is running BFD Version 0 and the other BFD neighbor is running Version 1, the session will run BFD Version 0. The output from the **show bfd neighbors** [**details**] command will verify which BFD version a BFD neighbor is running.

See the "Example: Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default" section on page 39-18 for an example of BFD version detection.

BFD Session Limits

The minimum number of BFD sessions that can be created varies with the "hello" interval. With "hello" intervals of 50ms, 128 sessions are permitted. More sessions are permitted at larger hello intervals.

BFD Support for Nonbroadcast Media Interfaces

Starting with Cisco IOS Release 15.1(1)SG, the BFD feature is supported on VLAN interfaces on the Catalyst 4500 series switch.

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

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 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 remain 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 switches (to provide redundancy), the switches have a graceful restart mechanism that protects the forwarding state during a switchover between the active RP and the standby RP.

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 switches.

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.

Timer values are different based on the number of BFD sessions and the platform.

Table 39-1 describes the timer value on Cisco 4500 series switches.

Table 39-1 BFD Timer Values on a Cisco 4500 Series Switches

Maximum Number of BFD Sessions	BFD Session Type	Minimum Timer Value (ms)	Clients	Comments
100	Async/echo	100 multiplier 3	All	A multiple of 5 is recommended for SSO switches.

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 establish successfully, 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.

BFD is supported on IPv4 and IPv6 static routes.

Note 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 the static route. This will cause the static route to remain in the RIB. The only workaround is to remove the static route BFD neighbor configuration so that the static route no longer tracks BFD session state.

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.

The closest alternative to BFD in conventional EIGRP, BGP, and OSPF deployments is the use of modified failure detection mechanisms for EIGRP, BGP, 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 BGP or OSPF, this Interior Gateway Protocol (IGP) protocol reduces its failure detection mechanism to a minimum of one second.

Advantages to implementing BFD over reduced timer mechanisms for routing protocols include the following:

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

Hardware Support for BFD

The Catalyst 4500 supports a limited number of BFD sessions in hardware. Placing a session in BFD hardware is termed *hardware offload*. The advantage of hardware offload is that session keep-alive is handled entirely in hardware, placing no load on the CPU.

Not all BFD sessions can be offloaded to hardware. The requirements for offloaded sessions are:

- BFD version 1
- IPv4
- No echo mode

The number of offloaded sessions varies by supervisor engine:

WS-X45-SUP6-E , WS-X45-SUP6L-E, WS-X4948-E, and C4900M, support 64 sessions in hardware. Further sessions must be supported in software.

WS-X45-SUP7-E, WS-X45-SUP7L-E, and WS-X45-SUP8-E support all 100 sessions in hardware.

The **show bfd neighbor detail** command displays print statistics for software and hardware (offloaded) sessions. Hardware sessions provide a limited set of statistics. In particular, statistics for packet transmit and receive intervals are not available for hardware sessions.

The **holddown** and **hello counts** are zero for all offloaded sessions.

Note Hardware offload is not supported for IPv6 BFD sessions.

How to Configure Bidirectional Forwarding Detection

You start a BFD process by configuring BFD on the interface. When the BFD process is started, no entries are created in the adjacency database; in other words, no BFD control packets are sent or received. BFD echo mode, which is supported in BFD Version 1, starting with Cisco IOS Release 15.1(1)SG, is enabled by default.

BFD echo packets are sent and received, in addition to BFD control packets. The adjacency creation takes places once you have configured BFD support for the applicable routing protocols. This section contains the following procedures:

- Configuring BFD Session Parameters on the Interface, page 39-8 (required)
- Configuring BFD Support for Dynamic Routing Protocols, page 39-9 (required)
- Configuring BFD Support for Static Routing, page 39-13 (optional)
- Configuring BFD Echo Mode, page 39-15 (optional)
- Monitoring and Troubleshooting BFD, page 39-17 (optional)

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.

To configure BFD session parameters, perform this task:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* `Switch(config)# interface gigabitethernet 6/1`	Enters interface configuration mode.
Step 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* `Switch(config-if)# bfd interval 100 min_rx 100 multiplier 3` `Switch(config-if)# no bfd echo`	Enables BFD on the interface. Disables BFD echo mode to enable Hardware Off-load.
Step 5	**end** `Switch(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, page 39-9 (optional)
- Configuring BFD Support for EIGRP, page 39-10 (optional)
- Configuring BFD Support for OSPF, page 39-11 (optional)

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.

Prerequisites

BGP must be running on all participating switches.

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 on page 39-8 for more information.

To configure BFD support for BGP, perform this task:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-tag* `Switch(config)# router bgp tag1`	Specifies a BGP process and enters router configuration mode.
Step 4	**neighbor** *ip-address* **fall-over bfd** `Switch(config-router)# neighbor 172.16.10.2 fall-over bfd`	Enables BFD support for fallover.
Step 5	**end** `Switch(config-router)# end`	Exits router configuration mode and returns the switch to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] `Switch# 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** `Switch# show ip bgp neighbor`	(Optional) Displays information about BGP and TCP connections to neighbors.

What to Do Next

See the "Monitoring and Troubleshooting BFD" section on page 39-17 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, page 39-10
- Configuring BFD Support for OSPF, page 39-11

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.

Prerequisites

EIGRP must be running on all participating switches.

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 on page 39-8 for more information.

To configure BFD support for EIGRP, perform this task:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**Switch eigrp** *as-number* `Switch(config)# router eigrp 123`	Configures the EIGRP routing process and enters router configuration mode.
Step 4	**bfd all-interfaces** or **bfd interface** *type number* `Switch(config-router)# bfd all-interfaces` or `Switch(config-router)# bfd interface gigabitethernet 6/1`	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** `Switch(config-router) end`	Exits router configuration mode and returns the switch to privileged EXEC mode.

	Command or Action	Purpose
Step 6	`show bfd neighbors [details]` `Switch# 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]` `Switch# 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 on page 39-17 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, page 39-11

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 on all 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 on 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, page 39-11 (optional)
- Configuring BFD Support for OSPF for One or More Interfaces, page 39-12 (optional)

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 on page 39-12.

Prerequisites

OSPF must be running on all participating switches.

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 on page 39-8 for more information.

To configure BFD support for OSPF for all interfaces:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**Switch ospf** *process-id* `Switch(config)# router ospf 4`	Specifies an OSPF process and enters router configuration mode.
Step 4	**bfd all-interfaces** `Switch(config-router)# bfd all-interfaces`	Enables BFD globally on all interfaces associated with the OSPF routing process.
Step 5	**end** `Switch(config-if)# end`	Exits interface configuration mode and returns the switch to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] `Switch# 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 7	**show ip ospf** `Switch# show ip ospf`	(Optional) Displays information that can help verify if BFD for OSPF has been enabled.

What to Do Next

See the "Monitoring and Troubleshooting BFD" section on page 39-17 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 BGP, page 39-9
- Configuring BFD Support for EIGRP, page 39-10

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 switches.

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 on page 39-8 for more information.

To configure BFD supporter for OSPF for one or more interfaces, perform this task:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* `Switch(config)# interface gigabitethernet 6/1`	Enters interface configuration mode.
Step 4	**ip ospf bfd** [**disable**] `Switch(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 switch configuration mode.
Step 5	**end** `Switch(config-if)# end`	Exits interface configuration mode and returns the switch to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] `Switch# 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. **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 displays the configured intervals, not the changed ones.
Step 7	**show ip ospf** `Switch# show ip ospf`	(Optional) Displays information that can help verify if BFD support for OSPF has been enabled.

What to Do Next

See the "Monitoring and Troubleshooting BFD" section on page 39-17 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 BGP, page 39-9
- Configuring BFD Support for EIGRP, page 39-10

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 on page 39-28.

To configure BFD support for static routing, perform this task:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* `Switch(config)# interface gigabitethernet6/1`	Configures an interface and enters interface configuration mode.
Step 4	**no switchport** `Switch(config-if)# no switchport`	Changes the interface to Layer 3.
Step 5	**ip address** *ip-address mask* `Switch(config-if)# ip address 10.201.201.1 255.255.255.0`	Configures an IP address for the interface.
Step 6	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* `Switch(config-if)# bfd interval 500 min_rx 500 multiplier 5`	Enables BFD on the interface.
Step 7	**exit** `Switch(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 8	**ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]] `Switch(config)# ip route static bfd Gi6/1 10.1.1.1 group group1 passive`	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 9	**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:** `Switch(config)# ip route 10.0.0.0 255.0.0.0 Gi6/1 10.201.201.2`	Specifies a static route BFD neighbor.
Step 10	**exit** **Example:** `Switch(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 11	**show ip static route** **Example:** `Switch# show ip static route`	(Optional) Displays static route database information.

	Command or Action	Purpose
Step 12	`show ip static route bfd` **Example:** `Switch# show ip static route bfd`	(Optional) Displays information about the static BFD configuration from the configured BFD groups and nongroup entries.
Step 13	`exit` **Example:** `Switch# 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 switches.

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, 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 on page 39-8 for more information.

Restrictions

BFD echo mode which is supported in BFD Version 1.

This section contains the following configuration tasks for BFD echo mode:

- Configuring the BFD Slow Timer, page 39-16
- Disabling BFD Echo Mode Without Asymmetry, page 39-16

Note BFD echo mode does not work in conjunction with Unicast Reverse Path Forwarding (uRPF) configuration. If BFD echo mode and uRPF configurations are enabled, then the sessions will flap.

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 switch.

To configure the BFD slow timer, perform this task:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**bfd slow-timer** *milliseconds* `Switch(config)# bfd slow-timer 12000`	Configures the BFD slow timer.
Step 4	**end** `Switch(config)# end`	Exits global configuration mode and returns the switch 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 are sent by the switch, and the switch does not forward BFD echo packets that are received from neighboring switches.

Repeat the steps in this procedure for each BFD switch.

To disable BFD echo mode without asymmetry, perform this task:

	Command or Action	Purpose
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	**interface** *type number* **Example:** `Switch(config)# interface GigabitEthernet 6/1`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**no bfd echo** **Example:** `Switch(config-if)# no bfd echo`	Disables BFD echo mode.
Step 5	**end** **Example:** `Switch(config-if)# end`	Exits global configuration mode and returns the switch to global configuration mode.

Monitoring and Troubleshooting BFD

This section describes how to retrieve BFD information for maintenance and troubleshooting. The commands in these tasks can be entered as needed, in any order.

For more information about BFD session initiation and failure, refer to the "BFD Operation" section on page 39-3.

To monitor and troubleshoot BFD, perform the following steps:

	Command or Action	Purpose
Step 1	**enable** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show bfd neighbors** [**details**] `Switch# show bfd neighbors details`	(Optional) Displays the BFD adjacency database. • The **details** keyword shows all BFD protocol parameters and timers per neighbor.
Step 3	**debug bfd** [**packet** | **event**] `Switch# debug bfd packet`	(Optional) Displays debugging information about BFD packets.

Configuration Examples for Bidirectional Forwarding Detection

This section provides the following configuration examples:

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

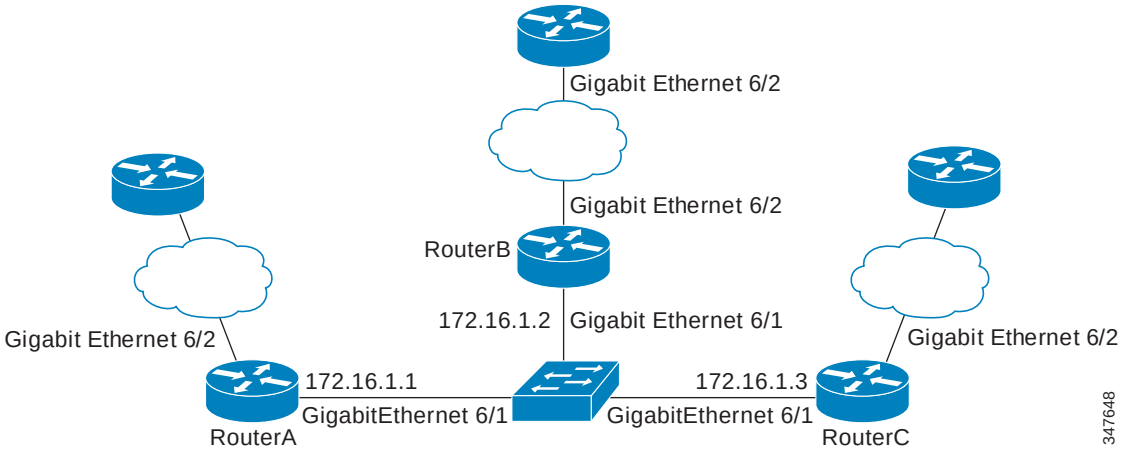
The following example shows how to configure BFD in an EIGRP network with echo mode enabled by default.

In this example, the EIGRP network contains SwitchA, SwitchB, and SwitchC. Gigabit Ethernet interface 6/1 on SwitchA is connected to the same network as Gigabit Ethernet interface 6/1 on SwitchB. Gigabit Ethernet interface 6/1 on SwitchB is connected to the same network as Gigabit Ethernet interface 6/1 on SwitchC.

SwitchA and SwitchB are running BFD Version 1, which supports echo mode, and SwitchC is running BFD Version 0, which does not support echo mode. We would say that the BFD sessions between SwitchC and its BFD neighbors are running echo mode with asymmetry. This is because echo mode will run on the forwarding path for RouteA and SwitchB, and their echo packets will return along the same path for BFD sessions and failure detections, while their BFD neighbor SwitchC runs BFD Version 0 and uses BFD controls packets for BFD sessions and failure detections.

Figure 39-3 shows a large EIGRP network with several switches, three of which are BFD neighbors that are running EIGRP as their routing protocol.

Figure 39-3 EIGRP Network with Three BFD Neighbors Running V1 or V0



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

Configuration for SwitchA

```
interface GigabitEthernet6/2
 no switch
 ip address 10.4.9.14 255.255.255.0
!
interface GigabitEthernet6/1
 no switchport
 ip address 172.16.1.1 255.255.255.0
 bfd interval 100 min_rx 50 multiplier 3
 no shutdown
!
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
!
```

Configuration for SwitchB

```
!
interface GigabitEthernet6/2
 no switchport
 ip address 10.4.9.34 255.255.255.0
!
interface GigabitEthernet6/1
 no switchport
 ip address 172.16.1.2 255.255.255.0
 bfd interval 100 min_rx 50 multiplier 3
!
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
!
```

Configuration for SwitchC

```
!
!
interface GigabitEthernet6/2
 no switchport
 no shutdown
 ip address 10.4.9.34 255.255.255.0
!
interface GigabitEthernet6/1
 no switchport
 ip address 172.16.1.3 255.255.255.0
 bfd interval 100 min_rx 50 multiplier 3
 no shutdown
!
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
!
!
end
```

The output from the **show bfd neighbors details** command from SwitchA verifies that BFD sessions have been created among all three switches and that EIGRP is registered for BFD support. The first group of output shows that SwitchC 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 SwitchB 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.

```
SwitchA

SwitchA# 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   Gi6/1
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(1364284)
Rx Count: 1351813, Rx Interval (ms) min/max/avg: 28/64/49 last: 4 ms ago
Tx Count: 1364289, Tx Interval (ms) min/max/avg: 40/68/49 last: 32 ms ago
Registered protocols: EIGRP
Uptime: 18:42:45
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 3          - Your Discr.: 5
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.1    172.16.1.2     6/1    Up        0    (3 )   Up        Gi6/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(317)
Rx Count: 305, Rx Interval (ms) min/max/avg: 1/1016/887 last: 448 ms ago
Tx Count: 319, Tx Interval (ms) min/max/avg: 1/1008/880 last: 532 ms ago
Registered protocols: EIGRP
Uptime: 00:04:30
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 1          - Your Discr.: 6
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

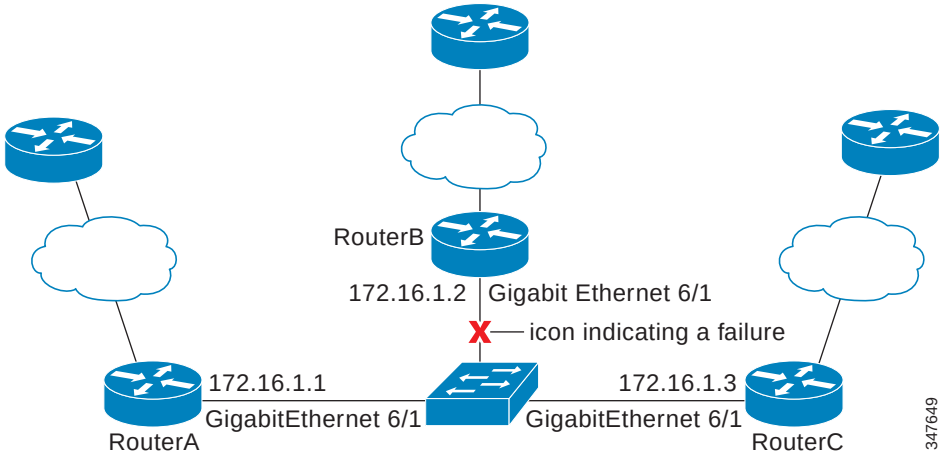
The output from the **show bfd neighbors details** command on SwitchB verifies that BFD sessions have been created and that EIGRP is registered for BFD support. As previously noted, SwitchA runs BFD Version 1, therefore echo mode is running, and SwitchC runs BFD Version 0, so echo mode does not run. The relevant command output is shown in bold.

```
SwitchB

SwitchB# 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        Gi6/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1             - Diagnostic: 0
             State bit: Up          - Demand bit: 0
             Poll bit: 0            - 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        Gi6/1
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(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
```

Figure 39-4 shows that Gigabit Ethernet interface 6/1 on SwitchB has failed. When Gigabit Ethernet interface 6/1 on SwitchB is shut down, the BFD values of the corresponding BFD sessions on SwitchA and SwitchB are reduced.

Figure 39-4 Gigabit Ethernet Interface 6/1 Failure



When Gigabit Ethernet interface 6/1 on SwitchB fails, BFD will no longer detect SwitchB as a BFD neighbor for SwitchA or for SwitchC. In this example, Gigabit Ethernet interface 6/1 has been administratively shut down on SwitchB.

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

```
SwitchA# 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        Gi6/1
```

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

```
SwitchC# 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        Gi6/1
```

Example: Configuring BFD in an OSPF Network

The following example shows how to configure BFD in an OSPF network.

In this example, the “simple” OSPF network consists of SwitchA and SwitchB. Gigabit Ethernet interface 6/1 on SwitchA is connected to the same network as Gigabit Ethernet interface 6/1 in SwitchB. The example, starting in global configuration mode, shows the configuration of BFD. For both SwitchA and SwitchB, BFD is configured globally for all interfaces associated with the OSPF process.

Configuration for SwitchA

```
!
interface GigabitEthernet 6/1
 no switchport
 ip address 172.16.10.1 255.255.255.0
 bfd interval 100 min_rx 100 multiplier 3
!
interface GigabitEthernet 6/2
 no switchport
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 SwitchB

```
!
interface GigabitEthernet 6/1
 no switchport
 ip address 172.16.10.2 255.255.255.0
 bfd interval 100 min_rx 100 multiplier 3
!
interface GigabitEthernet 6/2
 no switchport
 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.

SwitchA

```
SwitchA# 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        Gi6/1
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 on SwitchB verifies that a BFD session has been created:

SwitchB

```
SwitchB# attach 6

Switch> 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        Gi6/1
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.

SwitchA

```
SwitchA# show ip ospf

 Routing Process "ospf 123" with ID 172.16.10.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
 BFD is enabled
    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 00:00:08.828 ago
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x028417
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

SwitchB

```
SwitchB# show ip ospf

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

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

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

SwitchA

```
SwitchA# show ip ospf interface gigabitethernet 6/1

show ip ospf interface gigabitethernet 6/1
Gigabitethernet 6/1 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)
```

SwitchB

```
SwitchB# show ip ospf interface gigabitethernet 6/1

Gigabitethernet 6/1 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 Hardware-Offload support in a BGP Network Network

The following example shows how to configure BFD Hardware-Offload support in a BGP network.

In this example, the "simple" BGP network consists of SwitchA and SwitchB. Gigabit Ethernet interface 6/1 on SwitchA is connected to the same network as Gigabit Ethernet interface 6/1 in SwitchB.

Configuration for SwitchA

```
!
interface GigabitEthernet 6/1
 no switchport
 ip address 1.1.1.1 255.255.255.0
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo

router bgp 10
  neighbor 1.1.1.2 remote-as 10
  neighbor 1.1.1.2 fall-over bfd
!
```

Configuration for SwitchB

```
!
interface GigabitEthernet 6/1
 no switchport
 ip address 1.1.1.2 255.255.255.0
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo


router bgp 10
  neighbor 1.1.1.1 remote-as 10
  neighbor 1.1.1.1 fall-over bfd
!
```

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

SwitchA

```
SwitchA# show bfd neighbors details

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
1.1.1.1                                 1/1          Up        Up        Gi3/2
Session state is UP and not using echo function.
Session Host: Hardware
OurAddr: 1.1.1.2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 50(0)
Rx Count: 8678
Tx Count: 8680
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols:  BGP
Uptime: 00:06:18
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.: 1
             Min tx interval: 50000      - Min rx interval: 50000
             Min Echo interval: 0
```

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

SwitchB

```
SwitchB# attach 6

Switch> show bfd neighbors details

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
1.1.1.2                                 1/1          Up        Up        Gi1/2
Session state is UP and not using echo function.
Session Host: Hardware
OurAddr: 1.1.1.1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 50(0)
Rx Count: 10138
Tx Count: 10139
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: BGP
Uptime: 00:07:22
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.: 1
             Min tx interval: 50000     - Min rx interval: 50000
             Min Echo interval: 0
```

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

SwitchA

```
SwitchA# show ip bgp neighbors

BGP neighbor is 1.1.1.2,  remote AS 45000, external link
 Using BFD to detect fast fallover
..
```

SwitchB

```
SwitchB# show ip bgp neighbors

BGP neighbor is 1.1.1.1,  remote AS 40000, external link
 Using BFD to detect fast fallover
..
```

Example: Configuring BFD Support for Static Routing

In the following example, the network consists of SwitchA and SwitchB. Gigabit Ethernet interface 6/1 on SwitchA is connected to the same network as gigabit ethernet interface 6/1 on SwitchB. For the BFD session to come up, SwitchB must be configured.

SwitchA

```
configure terminal
 no switchport
 interface Gigabit Ethernet 6/1
 ip address 10.201.201.1 255.255.255.0
 bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Gigabit Ethernet 6/1 10.201.201.2
ip route 10.0.0.0 255.0.0.0 Gigabit Ethernet 6/1 10.201.201.2
```

SwitchB

```
configure terminal
 no switchport
 interface Gigabit Ethernet 6/1
 ip address 10.201.201.2 255.255.255.0
 bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Gigabit Ethernet 6/1 10.201.201.1
ip route 10.1.1.1 255.255.255.255 Gigabit Ethernet 6/1 10.201.201.1
```

Note The static route on SwitchB exists solely to enable the BFD session between 10.201.201.1 and 10.201.201.2. If there is no useful static route to configure, 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 Commands List, All Releases*
Configuring and monitoring BGP	Cisco BGP Overview" module of the *Cisco IOS IP Routing Protocols Configuration Guide*
Configuring and monitoring EIGRP	"Configuring EIGRP" module of the *Cisco IOS IP Routing Protocols Configuration Guide*
Configuring and monitoring OSPF	"Configuring OSPF" module of the *Cisco IOS IP Routing Protocols Configuration Guide*
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: Protocol-Independent Command Reference*

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

Standards

Standard	Title
IETF Draft	*BFD for IPv4 and IPv6 (Single Hop)*, February 2009
IETF Draft	*Bidirectional Forwarding Detection*, February 2009

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 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