



Configuring Bidirection Forwarding Detection

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Bidirectional Forwarding Detection, on page 1](#)
- [Restrictions for Bidirectional Forwarding Detection, on page 1](#)
- [Information About Bidirectional Forwarding Detection, on page 2](#)
- [How to Configure Bidirectional Forwarding Detection, on page 6](#)
- [Configuration Examples for Bidirectional Forwarding Detection, on page 19](#)

Finding Feature Information

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

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.

Prerequisites for Bidirectional Forwarding Detection

Prerequisites for BFD include:

- The switch's feature set is IP Base or higher. The IP Base feature set supports only Enhanced Interior Gateway Routing Protocol (EIGRP) stub routing, without BFD. The IP service feature set supports EIGRP with BFD.
- IP routing must be enabled on all participating switches
- Before BFD is deployed, configure one of the IP routing protocols supported by BFD on the switches. Also, implement fast convergence for the routing protocol that you plan to use.

Restrictions for Bidirectional Forwarding Detection

Restrictions for BFD include:

- BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away. Multihop configurations are not supported.
- The switch supports 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.
- To enable echo mode the peer system must be configured with the `no ip redirects` command.

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.

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.

This section includes the following subsections:

Related Topics

[Configuring BFD Echo Mode](#), on page 16

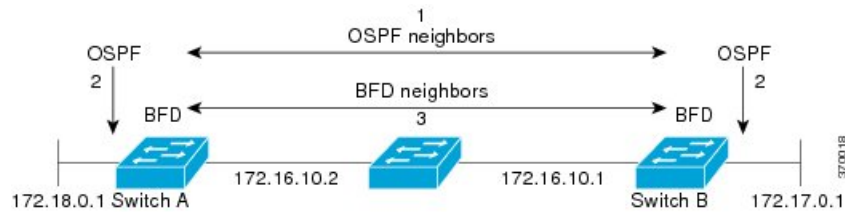
[Configuring BFD Session Parameters on the Interface](#), on page 6

[Monitoring and Troubleshooting BFD](#), on page 19

Neighbor Relationships

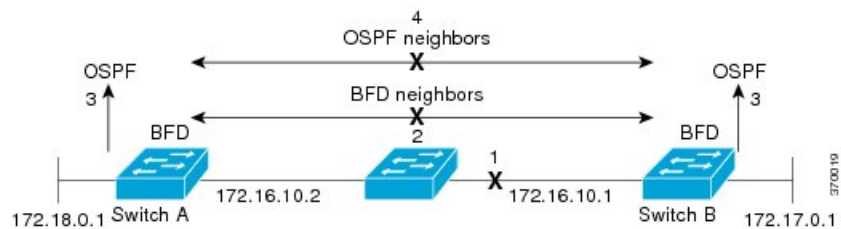
BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols BGP, EIGRP, IS-IS, and OSPF. By sending rapid failure detection notices to the routing protocols in the local router to initiate the routing table recalculation process, BFD contributes to greatly reduced overall network convergence time. The figure below shows a simple network with two routers running OSPF and BFD. When OSPF discovers a neighbor (1) it sends a request to the local BFD process to initiate a BFD neighbor session with the OSPF neighbor router (2). The BFD neighbor session with the OSPF neighbor router is established (3).

Figure 1: Establishing a BFD Neighbor Relationship



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.

Figure 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 routers in DROTHER state.

BFD Detection of Failures

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

- BFD is a forwarding path failure detection protocol. BFD detects a failure, but the routing protocol must take action to bypass a failed peer.
 - 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 protocol, 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

The 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.

Related Topics

[Example: Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default](#), on page 20

BFD Session Limits

The minimum number of BFD sessions that can be created varies with the “hello” interval. With “hello” intervals of 100ms, 100 sessions are permitted. More sessions are permitted at larger hello intervals. For a VLAN interface, the minimum “hello” interval is 600ms.

BFD Support for Nonbroadcast Media Interfaces

The BFD feature is supported on VLAN interfaces on the switch.

The **bfd interval** command must be configured on the 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 through intelligent line cards or dual forwarding processors while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and forwarding processors to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.

In devices that support dual RPs, SSO establishes one of the RPs as the active processor; the other RP is designated as the standby processor, and then synchronizes information between them. A switchover from the active to the standby processor occurs when the active RP fails, when it is removed from the networking device, or when it is manually taken down for maintenance.

BFD Support for Stateful Switchover

The BFD protocol provides short-duration detection of failures in the path between adjacent forwarding engines. In network deployments that use dual RP 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 1: BFD Timer Values on the switch

| 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 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 the static 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.

Related Topics

[Example: Configuring BFD Support for Static Routing](#), on page 29

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, 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, 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, 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.

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.

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

Perform this task to configure BFD on an interface by setting the baseline BFD session parameters on the interface. Repeat this task on 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. **no bfd echo**
6. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: Switch(config)# interface GigabitEthernet 6/1 | Specifies an interface type and number, and places the device in interface configuration mode. |
| Step 4 | bfd interval <i>milliseconds min_rx milliseconds multiplier interval-multiplier</i> Example: Switch(config-if)# no bfd echo | Enables BFD on the interface. Disables BFD echo mode to enable Hardware Off-load. |
| Step 5 | no bfd echo Example: Switch(config-if)# no bfd echo | Disables BFD echo mode to enable Hardware Off-load. |
| Step 6 | end Example: Switch(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |

Related Topics

- [Configuring BFD Echo Mode](#), on page 16
- [Configuring BFD Support for EIGRP](#), on page 9
- [Configuring BFD Support for BGP](#), on page 8
- [BFD Operation](#), on page 2
- [Configuring BFD Support for OSPF](#), on page 11
- [Configuring BFD Support for OSPF for One or More Interfaces](#), on page 13
- [Monitoring and Troubleshooting BFD](#), on page 19
- [Configuring BFD Support for OSPF for All Interfaces](#), on page 11

Configuring BFD Support for Dynamic Routing Protocols

You can enable BFD support for dynamic routing protocols at the device 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 tasks:

Configuring BFD Support for BGP

Perform this task to configure BFD support for Border Gateway Protocol (BGP) so that BGP is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD.

Before you begin

BGP must be running on all participating 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 for more information.



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

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|--------|--|---|
| Step 3 | router bgp <i>as-tag</i> Example: <pre>Switch(config)# router bgp tag1</pre> | Specifies a BGP process and enters router configuration mode. |
| Step 4 | neighbor <i>ip-address</i> fall-over bfd Example: <pre>Switch(config-router)# neighbor 172.16.10.2 fall-over bfd</pre> | Enables BFD support for fallover. |
| Step 5 | end Example: <pre>Switch(config-router)# end</pre> | Exits router configuration mode and returns to privileged EXEC mode. |
| Step 6 | show bfd neighbors [details] Example: <pre>Switch# show bfd neighbors detail</pre> | (Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. |
| Step 7 | show ip bgp neighbor Example: <pre>Switch# show ip bgp neighbor</pre> | (Optional) Displays information about BGP and TCP connections to neighbors. |

Related Topics

[Configuring BFD Session Parameters on the Interface](#), on page 6

[Monitoring and Troubleshooting BFD](#), on page 19

[Configuring BFD Support for OSPF for All Interfaces](#), on page 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.

Before you begin

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. For more information, see the "Configuring BFD Session Parameters on the Interface".

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 Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |
| Step 3 | router eigrp <i>as-number</i> Example: Switch(config)# router eigrp 123 | Configures the EIGRP routing process and enters router configuration mode. |
| Step 4 | Do one of the following: <ul style="list-style-type: none"> • bfd all-interfaces • bfd interface <i>type number</i> Example: Switch(config-router)# bfd all-interfaces Example: Switch(config-router)# bfd interface FastEthernet 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 Example: | Exits router configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Switch(config-router) end | |
| Step 6 | show bfd neighbors [details] Example: 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] Example: Switch# show ip eigrp interfaces detail | (Optional) Displays the interfaces for which BFD support for EIGRP has been enabled. |

Related Topics

- [Configuring BFD Support for OSPF](#), on page 11
- [Configuring BFD Session Parameters on the Interface](#), on page 6
- [Monitoring and Troubleshooting BFD](#), on page 19
- [Configuring BFD Support for OSPF for All Interfaces](#), on page 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 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:

Related Topics

- [Configuring BFD Support for EIGRP](#), on page 9
- [Configuring BFD Session Parameters on the Interface](#), on page 6
- [Monitoring and Troubleshooting BFD](#), on page 19
- [Configuring BFD Support for OSPF for All Interfaces](#), on page 11

Configuring BFD Support for OSPF for All Interfaces

Perform this task to configure BFD for all OSPF interfaces.

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 OSPF Support for BFD over IPv4 for One or More Interfaces](#) section.

Before you begin

Open Shortest Path First (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. For more information, see the “Configuring BFD Session Parameters on the Interface” section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **switch ospf *process-id***
4. **bfd all-interfaces**
5. **end**
6. **show bfd neighbors [details]**
7. **show ip ospf**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |
| Step 3 | switch ospf <i>process-id</i> Example: Switch(config)# router ospf 4 | Specifies an OSPF process and enters router configuration mode. |
| Step 4 | bfd all-interfaces Example: Switch(config-router)# bfd all-interfaces | Enables BFD globally on all interfaces associated with the OSPF routing process. |
| Step 5 | end Example: Switch(config-router)# end | Exits router configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 6 | show bfd neighbors [details] Example: <pre>Switch# show bfd neighbors detail</pre> | (Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. |
| Step 7 | show ip ospf Example: <pre>Switch# show ip ospf</pre> | (Optional) Displays information that can help verify if BFD for OSPF has been enabled. |

Related Topics

- [Configuring BFD Support for OSPF](#), on page 11
- [Configuring BFD Session Parameters on the Interface](#), on page 6
- [Configuring BFD Support for EIGRP](#), on page 9
- [Configuring BFD Support for BGP](#), on page 8
- [Configuring BFD Support for OSPF for One or More Interfaces](#), on page 13

Configuring BFD Support for OSPF for One or More Interfaces

Perform this task to configure BFD for all OSPF interfaces.

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 OSPF Support for BFD over IPv4 for One or More Interfaces](#) section.

Before you begin

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. For more information, see the “[Configuring BFD Session Parameters on the Interface](#)” section.

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: | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Switch> enable | |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |
| Step 3 | interface type number Example: Switch(config)# interface fastethernet 6/1 | (Optional) Enters interface configuration mode. |
| Step 4 | ip ospf bfd [disable] Example: Switch(config-if)# ip ospf bfd | (Optional) Enables or disables BFD on a per-interface basis for one or more interfaces associated with the OSPF routing process. Note 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 Example: Switch(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 6 | show bfd neighbors [details] Example: 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 Example: Switch# show ip ospf | (Optional) Displays information that can help verify if BFD for OSPF has been enabled. |

Related Topics

[Configuring BFD Session Parameters on the Interface](#), on page 6

[Monitoring and Troubleshooting BFD](#), on page 19

[Configuring BFD Support for OSPF for All Interfaces](#), on page 11

Configuring BFD Support for Static Routing

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no switchport**
5. **ip address** *ip-address mask*
6. **bfd interval** *milliseconds min_rx milliseconds multiplier interval-multiplier*
7. **exit**
8. **ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]]
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*]
10. **exit**
11. **show ip static route**
12. **show ip static route bfd**

DETAILED STEPS

| | 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 <i>type number</i> Example: Switch(config)# interface gigabitethernet 6/1 | Configures an interface and enters interface configuration mode. |
| Step 4 | no switchport Example: Switch(config)# no switchport | Changes the interface to Layer 3. |
| Step 5 | ip address <i>ip-address mask</i> Example: Switch(config-if)# ip address 10.201.201.1 255.255.255.0 | Configures an IP address for the interface. |
| Step 6 | bfd interval <i>milliseconds min_rx milliseconds multiplier interval-multiplier</i> Example: | Enables BFD on the interface. |

| | Command or Action | Purpose |
|----------------|---|--|
| | <pre>Switch(config-if)# bfd interval 500 min_rx 500 multiplier 5</pre> | |
| Step 7 | exit Example: <pre>Switch(config-if)# exit</pre> | Exits interface configuration mode and returns to global configuration mode. |
| Step 8 | ip route static bfd <i>interface-type interface-number ip-address</i> [group <i>group-name</i> [passive]] Example: <pre>Switch(config)# ip route static bfd serial 2/0 10.1.1.1 group group1 passive</pre> | Specifies a static route BFD neighbor. <ul style="list-style-type: none">• The <i>interface-type</i>, <i>interface-number</i>, and <i>ip-address</i> arguments are required because BFD support exists only for directly connected neighbors. |
| Step 9 | ip route [vrf <i>vrf-name</i>] <i>prefix mask</i> { <i>ip-address</i> <i>interface-type interface-number</i> [<i>ip-address</i>]} [dhcp] [<i>distance</i>] [name <i>next-hop-name</i>] [permanent track number] [tag <i>tag</i>] Example: <pre>Switch(config)# ip route 10.0.0.0 255.0.0.0 GigabitEthernet 6/1 10.201.201.2</pre> | Specifies a static route BFD neighbor. |
| Step 10 | exit Example: <pre>Switch(config)# exit</pre> | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 11 | show ip static route Example: <pre>Switch# show ip static route</pre> | (Optional) Displays static route database information. |
| Step 12 | show ip static route bfd Example: <pre>Switch# show ip static route bfd</pre> | (Optional) Displays information about the static BFD configuration from the configured BFD groups and non-group entries. |

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).

Related Topics

[Configuring BFD Session Parameters on the Interface](#), on page 6

[BFD Operation](#), on page 2

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, in order to avoid high CPU utilization.

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

Restrictions

BFD echo mode, which is supported in BFD Version 1.



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

This task show how to change the value of the BFD slow timer. Repeat the steps in this task for each BFD switch.

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| | Switch# configure terminal | |
| Step 3 | bfd slow-timer <i>milliseconds</i> Example: Switch(config)# bfd slow-timer 12000 | Configures the BFD slow timer. |
| Step 4 | end Example: Switch(config)# end | Exits global configuration mode and returns to privileged EXEC mode. |

Disabling BFD Echo Mode Without Asymmetry

This task shows how to disable BFD echo mode without asymmetry—no echo packets will be sent by the switch, and the switch will not forward BFD echo packets that are received from any neighbor switches.

Repeat the steps in this task for each BFD switch.

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |
| Step 3 | no bfd echo Example: Switch(config)# no bfd echo | Disables BFD echo mode. <ul style="list-style-type: none"> • Use the no form to disable BFD echo mode. |
| Step 4 | end Example: | Exits global configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|--|---------------------|---------|
| | Switch(config)# end | |

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.

To monitor and troubleshoot BFD, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **show bfd neighbors [details]**
3. **debug bfd [packet | event]**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show bfd neighbors [details] Example: Switch# show bfd neighbors details | (Optional) Displays the BFD adjacency database. <ul style="list-style-type: none"> • The details keyword shows all BFD protocol parameters and timers per neighbor. |
| Step 3 | debug bfd [packet event] Example: Switch# debug bfd packet | (Optional) Displays debugging information about BFD packets. |

Related Topics

- [Configuring BFD Session Parameters on the Interface](#), on page 6
- [Configuring BFD Support for EIGRP](#), on page 9
- [Configuring BFD Support for BGP](#), on page 8
- [BFD Operation](#), on page 2
- [Configuring BFD Support for OSPF](#), on page 11
- [Configuring BFD Support for OSPF for One or More Interfaces](#), on page 13

Configuration Examples for Bidirectional Forwarding Detection

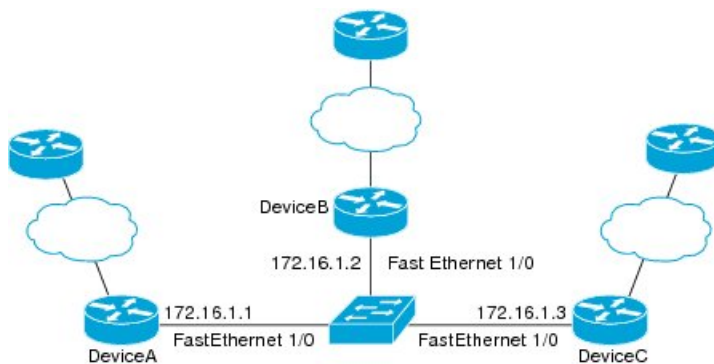
This section provides the following configuration examples:

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

In the following example, the EIGRP network contains DeviceA, DeviceB, and DeviceC. Fast Ethernet interface 1/0 on DeviceA is connected to the same network as Fast Ethernet interface 1/0 on Device B. Fast Ethernet interface 1/0 on DeviceB is connected to the same network as Fast Ethernet interface 1/0 on DeviceC.

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

The figure below shows a large EIGRP network with several devices, three of which are BFD neighbors that are running EIGRP as their routing protocol.



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

Configuration for DeviceA

```
interface Fast Ethernet0/0
no shutdown
ip address 10.4.9.14 255.255.255.0
duplex auto
speed auto
!
interface Fast Ethernet1/0
ip address 172.16.1.1 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
no shutdown
duplex auto
speed auto
!
router eigrp 11
network 172.16.0.0
bfd all-interfaces
auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
```

```
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
exec-timeout 30 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
!
end
```

Configuration for DeviceB

```
!
interface Fast Ethernet0/0
no shutdown
ip address 10.4.9.34 255.255.255.0
duplex auto
speed auto
!
interface Fast Ethernet1/0
ip address 172.16.1.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
no shtdown
duplex auto
speed auto
!
router eigrp 11
network 172.16.0.0
bfd all-interfaces
auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
exec-timeout 30 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
!
end
```

Configuration for DeviceC

```

!
!
interface Fast Ethernet0/0
no shutdown
ip address 10.4.9.34 255.255.255.0
duplex auto
speed auto
!
interface Fast Ethernet1/0
ip address 172.16.1.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
no shutdown
duplex auto
speed auto
!
router eigrp 11
network 172.16.0.0
bfd all-interfaces
auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
exec-timeout 30 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
!
end

```

The output from the **show bfd neighbors details** command from DeviceA verifies that BFD sessions are created among all three devices and that EIGRP is registered for BFD support. The first group of output shows that DeviceC 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 DeviceB with the IP address 172.16.1.2 runs BFD Version 1, and the 50 millisecond BFD interval parameter had been adopted. The relevant command output is shown in bold in the output.

```
DeviceA# show bfd neighbors details
```

```

OurAddr
      NeighAddr
      LD/RD  RH/RS  Holdown(mult)  State  Int
172.16.1.1  172.16.1.3
          5/3   1(RH)  150 (3 )         Up    Fa1/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0

```

```

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(1364284)
Rx Count: 1351813, Rx Interval (ms) min/max/avg: 28/64/49 last: 4 ms ago
Tx Count: 1364289, Tx Interval (ms) min/max/avg: 40/68/49 last: 32 ms ago
Registered protocols: EIGRP
Uptime: 18:42:45
Last packet: Version: 0
  - Diagnostic: 0
    I Hear You bit: 1      - Demand bit: 0
    Poll bit: 0           - Final bit: 0
    Multiplier: 3         - Length: 24
    My Discr.: 3          - Your Discr.: 5
    Min tx interval: 50000 - Min rx interval: 50000
    Min Echo interval: 0
OurAddr      NeighAddr
      LD/RD  RH/RS  Holdown(mult)  State      Int
172.16.1.1    172.16.1.2

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

```

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

```
DeviceB# 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      Fal/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1
  - Diagnostic: 0
    State bit: Up          - Demand bit: 0

```

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

```

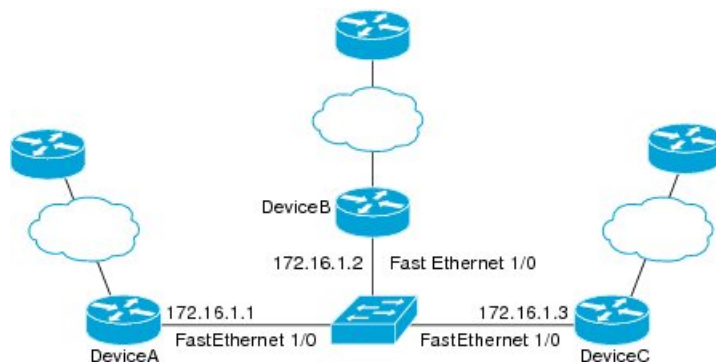
Poll bit: 0          - Final bit: 0
Multiplier: 3       - Length: 24
My Discr.: 6        - Your Discr.: 1
Min tx interval: 1000000 - Min rx interval: 1000000
Min Echo interval: 50000

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     Fa1/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(5735)
Rx Count: 5731, Rx Interval (ms) min/max/avg: 32/72/49 last: 32 ms ago
Tx Count: 5740, Tx Interval (ms) min/max/avg: 40/64/50 last: 44 ms ago
Registered protocols: EIGRP
Uptime: 00:04:45
Last packet: Version: 0
- Diagnostic: 0
I Hear You bit: 1 - Demand bit: 0
Poll bit: 0      - Final bit: 0
Multiplier: 3   - Length: 24
My Discr.: 6    - Your Discr.: 3
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0

```

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



When Fast Ethernet interface 1/0 on DeviceB fails, BFD will no longer detect Device B as a BFD neighbor for DeviceA or for DeviceC. In this example, Fast Ethernet interface 1/0 has been administratively shut down on DeviceB.

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

```

DeviceA# show bfd neighbors
OurAddr      NeighAddr

LD/RD RH/RS Holdown(mult) State Int
172.16.1.1 172.16.1.3
      5/3 1(RH) 134 (3 ) Up     Fa1/0

```


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

```
DeviceC# show bfd neighbors

OurAddr          NeighAddr

LD/RD RH  Holdown(mult)  State      Int
172.16.1.3   172.16.1.1
3/5  1  114 (3 )      Up         Fa1/0
```

Related Topics

[BFD Version Interoperability](#), on page 4

Example: Configuring BFD in an OSPF Network

The following example shows how to configure BFD in an OSPF network. In the following example, a simple OSPF network consists of Device A and Device B. Fast Ethernet interface 0/1 on Device A is connected to the same network as Fast Ethernet interface 6/0 in Device B. The example, starting in global configuration mode, shows the configuration of BFD. For both Devices A and B, BFD is configured globally for all interfaces associated with the OSPF process.

Configuration for Device A

```
!
interface Fast Ethernet 0/1
ip address 172.16.10.1 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
ip address 172.17.0.1 255.255.255.0
!
router ospf 123
log-adjacency-changes detail
network 172.16.0.0 0.0.0.255 area 0
network 172.17.0.0 0.0.0.255 area 0
bfd all-interfaces
```

Configuration for Device B

```
!
interface Fast Ethernet 6/0
ip address 172.16.10.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
ip address 172.18.0.1 255.255.255.0
!
router ospf 123
log-adjacency-changes detail
network 172.16.0.0 0.0.255.255 area 0
network 172.18.0.0 0.0.255.255 area 0
bfd all-interfaces
```

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

Device A

```
DeviceA# show bfd neighbors details
```

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

```
Uptime: 02:18:49
```

```
Last packet: Version: 0
```

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

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

Device B

```
DeviceB# attach 6
```

```
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
```

```
Device> show bfd neighbors details
```

```
Cleanup timer hits: 0
OurAddr      NeighAddr    LD/RD RH  Holdown(mult)  State    Int
172.16.10.2  172.16.10.1  8/1 1    1000 (5 )      Up       Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0      - Diagnostic: 0
I Hear You bit: 1          - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 5            - Length: 24
My Discr.: 1              - Your Discr.: 8
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
IPC Tx Failure Count: 0
IPC Rx Failure Count: 0
Total Adjs Found: 1
```

The output from the **show ip ospf** command verifies that BFD has been enabled for OSPF.

Device A

```
DeviceA# show ip ospf

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

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

Device B

```
DeviceB# show ip ospf

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

```

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 from the **show ip ospf interface** command verifies that BFD has been enabled for OSPF on the interfaces connecting Device A and Device B.

Device A

```

DeviceA# show ip ospf interface Fast Ethernet 0/1

show ip ospf interface Fast Ethernet 0/1
Fast Ethernet0/1 is up, line protocol is up
Internet Address 172.16.10.1/24, Area 0
Process ID 123, Router ID 172.16.10.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
Designated Router (ID) 172.18.0.1, Interface address 172.16.10.2
Backup Designated router (ID) 172.16.10.1, Interface address 172.16.10.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 172.18.0.1 (Designated Router)
Suppress hello for 0 neighbor(s)

```

Device B

```

DeviceB# show ip ospf interface Fast Ethernet 6/1

Fast Ethernet6/1 is up, line protocol is up
Internet Address 172.18.0.1/24, Area 0
Process ID 123, Router ID 172.18.0.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
Designated Router (ID) 172.18.0.1, Interface address 172.18.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec

```

```
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

Example: Configuring BFD Support for Static Routing

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

Device A

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

Device B

```
configure terminal
interface Serial 2/0
ip address 10.201.201.2 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.1
ip route 10.1.1.1 255.255.255.255 Serial 2/0 10.201.201.1
```

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

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

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

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

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

Related Topics

[BFD Support for Static Routing](#), on page 5

