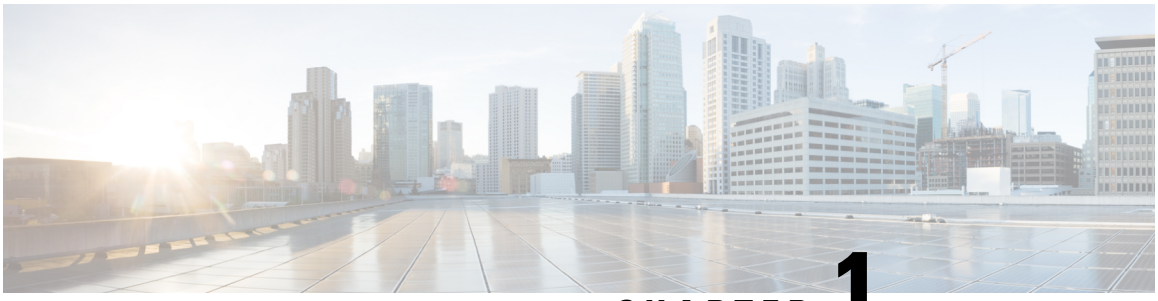
IP Routing: BFD Configuration Guide, Cisco IOS XE 17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

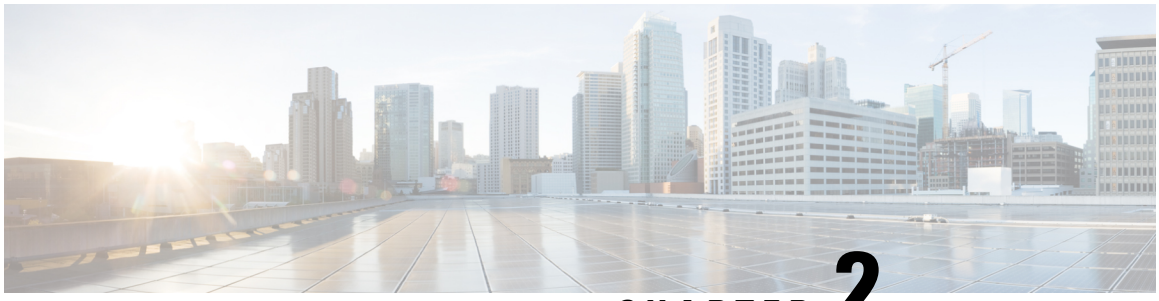
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.



CHAPTER 2

Bidirectional Forwarding Detection

This document describes how to enable the Bidirectional Forwarding Detection (BFD) protocol. BFD is a detection protocol that is designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. It includes a description of how to configure multihop BFD sessions.

BFD provides a consistent failure detection method for network administrators, in addition to fast forwarding path failure detection. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.

Finding Feature Information

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

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

Prerequisites for Bidirectional Forwarding Detection

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

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

Restrictions for Bidirectional Forwarding Detection

- When BFD is enabled on an interface, an ACL with "log" option is not supported on that interface.
- The Cisco IOS software incorrectly allows configuration of BFD on virtual-template and dialer interfaces; however, BFD functionality on virtual-template and dialer interfaces is not supported. Avoid configuring BFD on virtual-template and dialer interfaces.
- BFD is not supported on IPsec.
- BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away. Multihop configurations are not supported.
- BFD support is not available for all platforms and interfaces. To confirm BFD support for a specific platform or interface and obtain the most accurate platform and hardware restrictions, see the Cisco IOS software release notes for your software version.
- BFD packets are not matched in the QoS policy for self-generated packets.
- BFD packets are matched in the **class class-default** command. So, the user must make sure of the availability of appropriate bandwidth to prevent dropping of BFD packets due to oversubscription.
- BFD is not supported on VTI tunnel.
- BFD between peers goes down when the entry for the BFD control packets in the applied interface ACL has log keyword added as shown in the below example:

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

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

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

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

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

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

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

BFD support on DMVPN

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

Information About Bidirectional Forwarding Detection

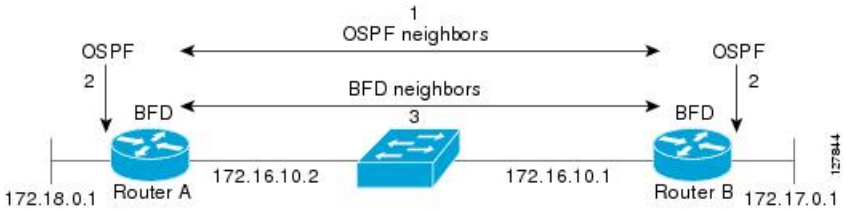
BFD Operation

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes.

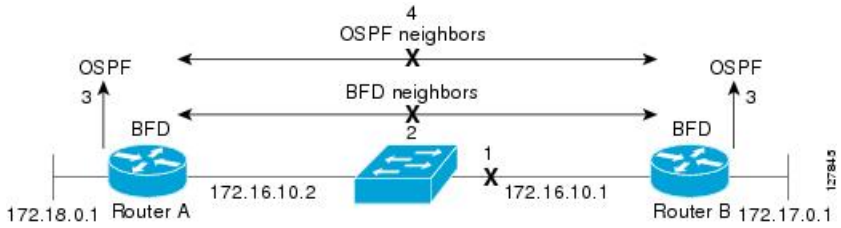
BFD is a detection protocol that is enabled at the interface and protocol levels. Cisco supports BFD asynchronous mode, which depends on the sending of BFD control packets between two systems to activate and maintain BFD neighbor sessions between routers. Therefore, in order for a BFD session to be created, BFD must be configured on both systems (or BFD peers). Once BFD has been enabled on the interfaces and at the router level for the appropriate protocols (NHRP and the routing protocol on overlay), a BFD session is created, BFD timers are negotiated, and the BFD peers will begin to send BFD control packets to each other at the negotiated interval.

Neighbor Relationships

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



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



A routing protocol needs to register with BFD for every neighbor it acquires. Once a neighbor is registered, BFD initiates a session with the neighbor if a session does not already exist.

OSPF registers with BFD when:

- A neighbor finite state machine (FSM) transitions to full state.
- Both OSPF BFD and BFD are enabled.

On broadcast interfaces, OSPF establishes a BFD session only with the designated router (DR) and backup designated router (BDR), but not between any two routers in DROTHER state.

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.

BFD Version Interoperability

All BFD sessions come up as Version 1 by default and will be interoperable with Version 0. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, if one BFD neighbor is running BFD Version 0 and the other BFD neighbor is running Version 1, the session will run BFD Version 0. The output from the **show bfd neighbors** [**details**] command will verify which BFD version a BFD neighbor is running.

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

BFD Support for Nonbroadcast Media Interfaces

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

BFD Support for VPN Routing and Forwarding Interfaces

The BFD feature is extended

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

BFD Support for Nonstop Forwarding with Stateful Switchover

Typically, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in a routing flap, which could spread across multiple routing

domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Nonstop forwarding (NSF) helps to suppress routing flaps in devices that are enabled with stateful switchover (SSO), thereby reducing network instability.

NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored after a switchover. With NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and forwarding processors to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.

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

BFD Support for Stateful Switchover

The BFD protocol provides short-duration detection of failures in the path between adjacent forwarding engines. In network deployments that use dual RP routers or switches (to provide redundancy), the routers have a graceful restart mechanism that protects the forwarding state during a switchover between the active RP and the standby RP.

The dual RPs have variable switchover times that depend on the ability of the hardware to detect a communication failure. When BFD is running on the RP, some platforms are not able to detect a switchover before the BFD protocol times out; these platforms are referred to as slow switchover platforms.

Stateful BFD on the Standby RP

To ensure a successful switchover to the standby RP, the BFD protocol uses checkpoint messages to send session information from the active RP Cisco IOS instance to the standby RP Cisco IOS instance. The session information includes local and remote discriminators, adjacent router timer information, BFD setup information, and session-specific information such as the type of session and the session version. In addition, the BFD protocol sends session creation and deletion checkpoint messages to create or delete a session on the standby RP.

The BFD sessions on the standby RP do not receive or send packets and do not process expired timers. These sessions wait for a switchover to occur and then send packets for any active sessions so that sessions do not time out on adjacent routers.

When the BFD protocol on the standby RP is notified of a switchover it changes its state to active, registers itself with Cisco Express Forwarding so that it can receive packets, and then sends packets for any elements that have expired.

BFD also uses checkpoint messages to ensure that sessions created by clients on the active RP are maintained during a switchover. When a switchover occurs, BFD starts an SSO reclaim timer. Clients must reclaim their sessions within the duration specified by the reclaim timer or else the session is deleted.

BFD Support for Static Routing

Unlike dynamic routing protocols, such as OSPF and BGP, static routing has no method of peer discovery. Therefore, when BFD is configured, the reachability of the gateway is completely dependent on the state of the BFD session to the specified neighbor. Unless the BFD session is up, the gateway for the static route is considered unreachable, and therefore the affected routes will not be installed in the appropriate Routing Information Base (RIB).

For a BFD session to be successfully established, BFD must be configured on the interface on the peer and there must be a BFD client registered on the peer for the address of the BFD neighbor. When an interface is used by dynamic routing protocols, the latter requirement is usually met by configuring the routing protocol instances on each neighbor for BFD. When an interface is used exclusively for static routing, this requirement must be met by configuring static routes on the peers.

If a BFD configuration is removed from the remote peer while the BFD session is in the up state, the updated state of the BFD session is not signaled to IPv4 static. This will cause the static route to remain in the RIB. The only workaround is to remove the IPv4 static BFD neighbor configuration so that the static route no longer tracks BFD session state. Also, if you change the encapsulation type on a serial interface to one that is unsupported by BFD, BFD will be in a down state on that interface. The workaround is to shut down the interface, change to a supported encapsulation type, and then reconfigure BFD.

A single BFD session can be used by an IPv4 static client to track the reachability of next hops through a specific interface. You can assign a BFD group for a set of BFD-tracked static routes. Each group must have one active static BFD configuration, one or more passive BFD configurations, and the corresponding static routes to be BFD-tracked. Nongroup entries are BFD-tracked static routes for which a BFD group is not assigned. A BFD group must accommodate static BFD configurations that can be part of different VRFs. Effectively, the passive static BFD configurations need not be in the same VRF as that of the active configuration.

For each BFD group, there can be only one active static BFD session. You can configure the active BFD session by adding a static BFD configuration and a corresponding static route that uses the BFD configuration. The BFD session in a group is created only when there is an active static BFD configuration and the static route that uses the static BFD configuration. When the active static BFD configuration or the active static route is removed from a BFD group, all the passive static routes are withdrawn from the RIB. Effectively, all the passive static routes are inactive until an active static BFD configuration and a static route to be tracked by the active BFD session are configured in the group.

Similarly, for each BFD group, there can be one or more passive static BFD configurations and their corresponding static routes to be BFD-tracked. Passive static session routes take effect only when the active BFD session state is reachable. Though the active BFD session state of the group is reachable, the passive static route is added to the RIB only if the corresponding interface state is up. When a passive BFD session is removed from a group, it will not affect the active BFD session if one existed, or the BFD group reachability status.

BFD on Multiple Hops

BFD is supported

on arbitrary paths, which might span multiple network hops. The BFD Multihop feature provides subsecond forwarding failure detection for a destination more than one hop, and up to 255 hops, away.

A BFD multihop session is set up between a unique source-destination address pair provided by the client. A session can be set up between two endpoints that have IP connectivity.

You must configure the **bfd-template** and **bfd map** commands to create a multihop template and associate it with one or more maps of destinations and associated BFD timers. You can enable authentication and configure a key chain for BFD multihop sessions.

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

Benefits of Using BFD for Failure Detection

When you deploy any feature, it is important to consider all the alternatives and be aware of any trade-offs being made.

The closest alternative to BFD in conventional EIGRP, IS-IS, and OSPF deployments is the use of modified failure detection mechanisms for EIGRP, IS-IS, and OSPF routing protocols.

If you set EIGRP hello and hold timers to their absolute minimums, the failure detection rate for EIGRP falls to within a one- to two-second range.

If you use fast hellos for either IS-IS or OSPF, these Interior Gateway Protocol (IGP) protocols reduce their failure detection mechanisms to a minimum of one second.

There are several advantages to implementing BFD over reduced timer mechanisms for routing protocols:

- Although reducing the EIGRP, IS-IS, and OSPF timers can result in minimum detection timer of one to two seconds, BFD can provide failure detection in less than one second.
- Because BFD is not tied to any particular routing protocol, it can be used as a generic and consistent failure detection mechanism for EIGRP, IS-IS, and OSPF.
- Because some parts of BFD can be distributed to the data plane, it can be less CPU-intensive than the reduced EIGRP, IS-IS, and OSPF timers, which exist wholly at the control plane.

Benefits of BFD Support on DMVPN

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

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

How to Configure Bidirectional Forwarding Detection

Configuring BFD Session Parameters on the Interface

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

SUMMARY STEPS

1. **enable**

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

DETAILED STEPS

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

Step 3	Perform one of the following steps:
	• **ip address** *ipv4-address mask*
	• **ipv6 address** *ipv6-address*/*mask*
	Example:
	Configuring an IPv4 address for the interface:
	`Device(config-if)# ip address 10.201.201.1 255.255.255.0`
	Configuring an IPv6 address for the interface:
	`Device(config-if)# ipv6 address 2001:db8:1:1::1/32`
		Configures an IP address for the interface.

Step 4	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring BFD Support for Dynamic Routing Protocols

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

This section describes the following procedures:

Configuring BFD Support for BGP

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

Before you begin

BGP must be running on all participating routers.

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-tag* **Example:** `Router(config)# router bgp tag1`	Specifies a BGP process and enters router configuration mode.
Step 4	**neighbor** *ip-address* **fall-over bfd** **Example:**	Enables BFD support for fallover.

	Command or Action	Purpose
	`Router(config-router)# neighbor 172.16.10.2 fall-over bfd`	
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns the router to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors detail`	(Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.
Step 7	**show ip bgp neighbor** **Example:** `Router# 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 for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections.

Configuring BFD Support for EIGRP

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

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

Before you begin

EIGRP must be running on all participating routers.

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 123`	Configures the EIGRP routing process and enters router configuration mode.

Step 4	Do one of the following:
	• **bfd all-interfaces**
	• **bfd interface** *type number*
	Example:
	`Router(config-router)# bfd all-interfaces`
	Example:
	`Router(config-router)# bfd interface FastEthernet 6/0`
		Enables BFD globally on all interfaces associated with the EIGRP routing process.
		or
		Enables BFD on a per-interface basis for one or more interfaces associated with the EIGRP routing process.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-router) end`	Exits router configuration mode and returns the router to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	(Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.
Step 7	**show ip eigrp interfaces** [*type number*] [*as-number*] [**detail**] **Example:** `Router# show ip eigrp interfaces detail`	(Optional) Displays the interfaces for which BFD support for EIGRP has been enabled.

What to Do Next

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

Configuring BFD Support for IS-IS

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

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

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

Prerequisites

IS-IS must be running on all participating routers.

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

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

Configuring BFD Support for IS-IS for All Interfaces

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis tag1`	Specifies an IS-IS process and enters router configuration mode.
Step 4	**bfd all-interfaces** **Example:** `Router(config-router)# bfd all-interfaces`	Enables BFD globally on all interfaces associated with the IS-IS routing process.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-router)# exit`	(Optional) Returns the router to global configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastethernet 6/0`	(Optional) Enters interface configuration mode.
Step 7	**ip router isis** [*tag*] **Example:** `Router(config-if)# ip router isis tag1`	(Optional) Enables support for IPv4 routing on the interface.
Step 8	**isis bfd** [**disable**] **Example:** `Router(config-if)# isis bfd`	(Optional) Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. **Note** You should use the **disable** keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the **bfd all-interfaces** command in router configuration mode.
Step 9	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 10	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	(Optional) Displays information that can be used to verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.
Step 11	**show clns interface** **Example:** `Router# show clns interface`	(Optional) Displays information that can be used to verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

What to Do Next

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 6/0`	Enters interface configuration mode.
Step 4	**ip router isis** [*tag*] **Example:** `Router(config-if)# ip router isis tag1`	Enables support for IPv4 routing on the interface.

	Command or Action	Purpose
Step 5	**isis bfd [disable]** **Example:** `Router(config-if)# isis bfd`	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. **Note** You should use the **disable** keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the **bfd all-interfaces** command in router configuration mode.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 7	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.
Step 8	**show clns interface** **Example:** `Router# show clns interface`	(Optional) Displays information that can help verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

What to Do Next

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

Configuring BFD Support for OSPF

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

There are two methods for enabling BFD support for OSPF:

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

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

Configuring BFD Support for OSPF for All Interfaces

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

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

Before you begin

OSPF must be running on all participating routers.

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:**	Specifies an OSPF process and enters router configuration mode.

	Command or Action	Purpose
	`Router(config)# router ospf 4`	
Step 4	**bfd all-interfaces** [**strict-mode**] **Example:** `Router(config-router)# bfd all-interfaces`	Enables BFD globally on all interfaces associated with the OSPF routing process. **[strict-mode]** - BFD session is established in the strict-mode. In the strict-mode, the OSPF session is not established till the BFD session is established.
Step 5	**exit** **Example:** `Router(config-router)# exit`	(Optional) Returns the router to global configuration mode. Enter this command only if you want to perform Step 7 to disable BFD for one or more interfaces.
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastethernet 6/0`	(Optional) Enters interface configuration mode. Enter this command only if you want to perform Step 7 to disable BFD for one or more interfaces.
Step 7	**ip ospf bfd** [**disable**] **Example:** `Router(config-if)# ip ospf bfd disable`	(Optional) Disables BFD on a per-interface basis for one or more interfaces associated with the OSPF routing process. **Note** You should use the **disable** keyword only if you enabled BFD on all of the interfaces that OSPF is associated with using the **bfd all-interfaces** command in router configuration mode.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 9	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors detail`	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.
Step 10	**show ip ospf** **Example:** `Router# show ip ospf`	(Optional) Displays information that can help verify if BFD for OSPF has been enabled. If BFD is enabled in strict-mode, the command output displays `BFD is enabled in strict mode.`

What to Do Next

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

Configuring BFD Support for OSPF for One or More Interfaces

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

Before you begin

OSPF must be running on all participating routers.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 6/0`	Enters interface configuration mode.
Step 4	**ip ospf bfd** [**disable**] [**strict-mode**] **Example:** `Router(config-if)# ip ospf bfd`	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the OSPF routing process. **Note** You should use the **disable** keyword only if you enabled BFD on all of the interfaces that OSPF is associated with using the **bfd all-interfaces** command in router configuration mode.

	Command or Action	Purpose
		[strict-mode] - BFD session is established in the strict-mode. In the strict-mode, the OSPF session is not established till the BFD session is established.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** If hardware-offloaded BFD sessions are configured with Tx and Rx intervals that are not multiples of 50 ms, the hardware intervals are changed. However, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.
Step 7	**show ip ospf** **Example:** `Router# show ip ospf`	(Optional) Displays information that can help verify if BFD support for OSPF has been enabled. If BFD is enabled in strict-mode, the command output displays `BFD is enabled in strict mode.`

What to Do Next

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

Configuring BFD Support for HSRP

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

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

Before you begin

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]

4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **standby bfd**
8. **exit**
9. **standby bfd all-interfaces**
10. **exit**
11. **show standby neighbors**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** [**distributed**] **Example:** `Router(config)# ip cef`	Enables Cisco Express Forwarding or distributed Cisco Express Forwarding.
Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 6/0`	Enters interface configuration mode.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.11 255.255.255.0`	Configures an IP address for the interface.
Step 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.11`	Activates HSRP.
Step 7	**standby bfd** **Example:** `Router(config-if)# standby bfd`	(Optional) Enables HSRP support for BFD on the interface.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 9	**standby bfd all-interfaces** **Example:** `Router(config)# standby bfd all-interfaces`	(Optional) Enables HSRP support for BFD on all interfaces.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 11	**show standby neighbors** **Example:** `Router# show standby neighbors`	(Optional) Displays information about HSRP support for BFD.

What to Do Next

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

Configuring BFD Support for Static Routing

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Perform one of the following steps:
   - **ip address** *ipv4-address mask*
   - **ipv6 address** *ipv6-address*/*mask*
5. **exit**
6. Perform one of the following steps:
   - **ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]]
   - **ipv6 route static bfd** *interface-type interface-number ip-address* [**unaasosiated**]
7. Perform one of the following steps:

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

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface`	Configures an interface and enters interface configuration mode.

Step 4	Perform one of the following steps:
	• **ip address** *ipv4-address mask*
	• **ipv6 address** *ipv6-address*/*mask*
	Example:
	Configuring an IPv4 address for the interface:
	`Device(config-if)# ip address 10.201.201.1 255.255.255.0`
	Configuring an IPv6 address for the interface:
	`Device(config-if)# ipv6 address 2001:db8:1:1::1/32`
		Configures an IP address for the interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Step 6	Perform one of the following steps:
	• **ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]]
	• **ipv6 route static bfd** *interface-type interface-number ip-address* [**unaasosiated**]
	Example:
	`Device(config)# ip route static bfd 10.1.1.1 group group1 passive`
	`Device(config)# ipv6 route static bfd TenGigabitEthernet 0/0/7 19:1:1::2`
		Specifies a static route BFD neighbor.
		• The *interface-type*, *interface-number*, and *ip-address* arguments are required because BFD support exists only for directly connected neighbors.

Step 7	Perform one of the following steps:
	• **ip route** [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
	• **ipv6 route** [**vrf** *vrf-name*] *ipv6 prefix*/*mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**name** *next-hop-name*] [**track** *number*] [**tag** *tag*]
	Example:
	`Device(config)# ip route 10.0.0.0 255.0.0.0`
	`Device(config)# ipv6 route 19:1:1::/64 TenGigabitEthernet0/0/7 19:1:1::2`
		Specifies a static route BFD neighbor.

Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	Perform one of the following steps: • **show ip static route** • **show ipv6 static** **Example:**	(Optional) Displays static route database information.

	Command or Action	Purpose
Step 10	Perform one of the following steps: • **show ip static route bfd** • **show ipv6 static bfd** **Example:**	(Optional) Displays information about the static BFD configuration from the configured BFD groups and nongroup entries.
Step 11	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode and returns to user EXEC mode.

Configuring BFD Echo Mode

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

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

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

Prerequisites

BFD must be running on all participating routers.

Before using BFD echo mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the **no ip icmp redirects** command, in order to avoid high CPU utilization.

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

Restrictions

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

Configuring the BFD Slow Timer

The steps in this procedure show how to change the value of the BFD slow timer. Repeat the steps in this procedure for each BFD router.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**bfd slow-timer** *milliseconds* **Example:** `Switch(config)# bfd slow-timer 12000`	Configures the BFD slow timer.
Step 4	**end** **Example:** `Switch(config)# end`	Exits global configuration mode and returns the router to privileged EXEC mode.

Disabling BFD Echo Mode Without Asymmetry

The steps in this procedure show how to disable BFD echo mode without asymmetry—no echo packets will be sent by the router, and the router will not forward BFD echo packets that are received from any neighbor routers.

Repeat the steps in this procedure for each BFD router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Creating and Configuring BFD Templates

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

Configuring a Single-Hop Template

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bfd-template single-hop** *template-name* **Example:**	Creates a single-hop BFD template and enters BFD configuration mode.

	Command or Action	Purpose
	`Router(config)# bfd-template single-hop bfdtemplate1`	
Step 4	**interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value* **Example:** `Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3`	Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.
Step 5	**end** **Example:** `Router(bfd-config)# end`	Exits BFD configuration mode and returns the router to privileged EXEC mode.

Configuring a Multihop Template

Perform this task to create a BFD multihop template and configure BFD interval timers, authentication, and key chain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bfd-template multi-hop** *template-name*
4. **interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value*
5. **authentication** *authentication-type* **keychain** *keychain-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bfd-template multi-hop** *template-name* **Example:** `Router(config)# bfd-template multi-hop mh-template1`	Creates a BFD multihop BFD template and enters BFD configuration mode.

	Command or Action	Purpose
Step 4	**interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value* **Example:** `Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3`	Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.
Step 5	**authentication** *authentication-type* **keychain** *keychain-name* **Example:** `Router(bfd-config)# authentication keyed-sha-1 keychain bfd-multihop`	Configures authentication for the multihop template and specifies the authentication type.
Step 6	**end** **Example:** `Router(bfd-config)# end`	Exits BFD configuration mode and returns the router to privileged EXEC mode.

Configuring BFD Support on DMVPN

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

```
enable
configure terminal
interface tunnel1
bfd interval 1000 min_rx 1000 multiplier 5
no echo
```

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

```
enable
configure terminal
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 5
interface tunnel1
bfd template sample
```

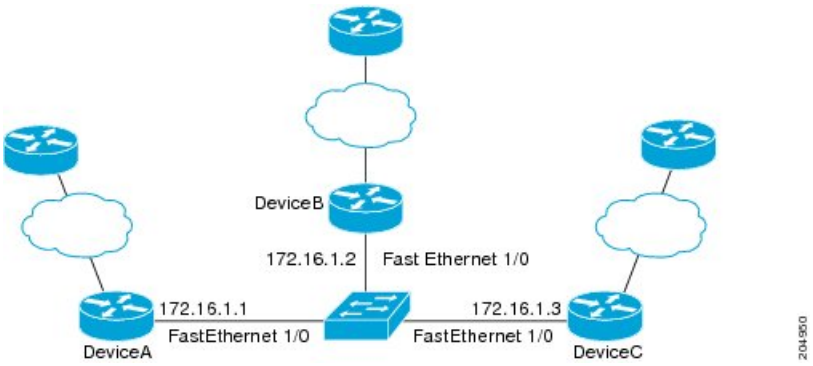
Configuration Examples for Bidirectional Forwarding Detection

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

In the following example, the EIGRP network contains RouterA, RouterB, and RouterC. Fast Ethernet interface 1/0 on RouterA is connected to the same network as Fast Ethernet interface 1/0 on Router B. Fast Ethernet interface 1/0 on RouterB is connected to the same network as Fast Ethernet interface 1/0 on RouterC.

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

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



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

Configuration for RouterA

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

```
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
 exec-timeout 30 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

Configuration for RouterB

```
!
interface Fast Ethernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface Fast Ethernet1/0
 ip address 172.16.1.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 no 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 RouterC

```
!
!
interface Fast Ethernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface Fast Ethernet1/0
 ip address 172.16.1.3 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 no shutdown
 duplex auto
 speed auto
!
router eigrp 11
 network 172.16.0.0
 bfd all-interfaces
 auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
 exec-timeout 30 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

The output from the **show bfd neighbors details** command from RouterA verifies that BFD sessions have been created among all three routers and that EIGRP is registered for BFD support. The first group of output shows that RouterC with the IP address 172.16.1.3 runs BFD Version 0 and therefore does not use the echo mode. The second group of output shows that RouterB with the IP address 172.16.1.2 does run BFD Version 1, and the 50 millisecond BFD interval parameter had been adopted. The relevant command output is shown in bold in the output.

```
RouterA# show bfd neighbors details

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

```
     5/3    1(RH)    150 (3 )       Up   Fa1/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(1364284)
Rx Count: 1351813, Rx Interval (ms) min/max/avg: 28/64/49 last: 4 ms ago
Tx Count: 1364289, Tx Interval (ms) min/max/avg: 40/68/49 last: 32 ms ago
Registered protocols: EIGRP
Uptime: 18:42:45
Last packet: Version: 0
            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 3          - Your Discr.: 5
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0
OurAddr       NeighAddr
     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.1    172.16.1.2

    6/1    Up        0    (3 )   Up        Fa1/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(317)
Rx Count: 305, Rx Interval (ms) min/max/avg: 1/1016/887 last: 448 ms ago
Tx Count: 319, Tx Interval (ms) min/max/avg: 1/1008/880 last: 532 ms ago
Registered protocols: EIGRP
Uptime: 00:04:30
Last packet: Version: 1

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

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

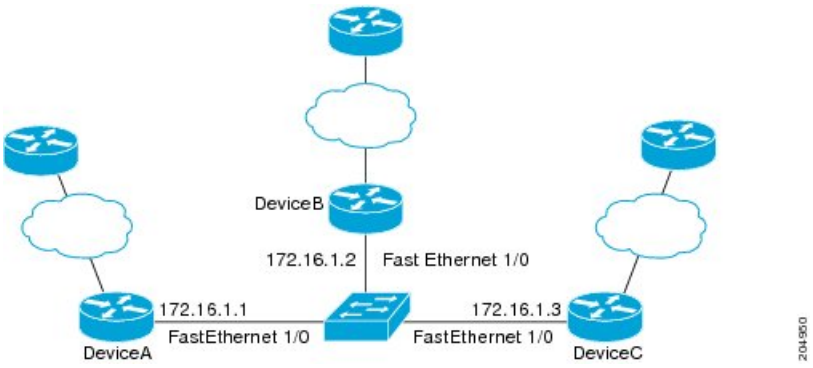
```
RouterB# show bfd neighbors details

OurAddr       NeighAddr
     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.1
    1/6    Up        0    (3 )   Up        Fa1/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
```

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



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

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

```
RouterA# show bfd neighbors
OurAddr       NeighAddr

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

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

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

```
RouterC# show bfd neighbors

OurAddr       NeighAddr

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

    3/5  1   114  (3 )      Up        Fa1/0
```

Example: Configuring BFD in an OSPF Network

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

Configuration for Router A

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

Configuration for Router B

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

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

Router A

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


Uptime: 02:18:49
Last packet: Version: 0
            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 2          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

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

Router B

```
RouterB# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0           - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

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

Router A

```
RouterA# show ip ospf

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


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

Router B

```
RouterB# show ip ospf

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

```
 Number of areas transit capable is 0
 External flood list length 0
 BFD is enabled


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

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

Router A

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

Router B

```
RouterB# show ip ospf interface Fast Ethernet 6/1
Fast Ethernet6/1 is up, line protocol is up
  Internet Address 172.18.0.1/24, Area 0
  Process ID 123, Router ID 172.18.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
  Designated Router (ID) 172.18.0.1, Interface address 172.18.0.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Example: Configuring BFD in a BGP Network

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

Configuration for Router A

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

Configuration for Router B

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

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

Router A

```
RouterA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/8  1   332  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(15491)
Rx Count: 9160, Rx Interval (ms) min/max/avg: 200/440/332 last: 268 ms ago
Tx Count: 15494, Tx Interval (ms) min/max/avg: 152/248/197 last: 32 ms ago
Registered protocols: BGP
Uptime: 00:50:45
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 8          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

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

Router B

```
RouterB# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

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

Router A

```
RouterA# show ip bgp neighbors
BGP neighbor is 172.16.10.2,  remote AS 45000, external link
 Using BFD to detect fast fallover
.
.
.
```

Router B

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

Example: Configuring BFD in an IS-IS Network

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

Configuration for Router A

```
!
interface Fast Ethernet 0/1
 ip address 172.16.10.1 255.255.255.0
ip router isis
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
ip address 172.17.0.1 255.255.255.0
ip router isis
!
router isis
 net 49.0001.1720.1600.1001.00
 bfd all-interfaces
!
```

Configuration for Router B

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

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

```
RouterA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/8  1   536  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(23543)
Rx Count: 13877, Rx Interval (ms) min/max/avg: 200/448/335 last: 64 ms ago
Tx Count: 23546, Tx Interval (ms) min/max/avg: 152/248/196 last: 32 ms ago
Registered protocols: ISIS
Uptime: 01:17:09
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 8          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

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

```
RouterB# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

Example: Configuring BFD in an HSRP Network

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

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

Router A

```
ip cef
interface Fast Ethernet2/0
 no shutdown
 ip address 10.0.0.2 255.0.0.0
 ip router-cache cef
 bfd interval 200 min_rx 200 multiplier 3
 standby 1 ip 10.0.0.11
 standby 1 preempt
 standby 1 priority 110

 standby 2 ip 10.0.0.12
 standby 2 preempt
 standby 2 priority 110
```

Router B

```
interface Fast Ethernet2/0
 ip address 10.1.0.22 255.255.0.0
 no shutdown
 bfd interval 200 min_rx 200 multiplier 3
 standby 1 ip 10.0.0.11
 standby 1 preempt
 standby 1 priority 90
 standby 2 ip 10.0.0.12
 standby 2 preempt
 standby 2 priority 80
```

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

```
RouterA#show standby neighbors

HSRP neighbors on Fast Ethernet2/0
  10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !
RouterB# show standby neighbors

HSRP neighbors on Fast Ethernet2/0
  10.0.0.2
    Active groups: 1
```

```
No standby groups
BFD enabled !
```

Example: Configuring BFD Support for Static Routing

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

Device A

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

Device B

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

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

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

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

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

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

Example: BFD Support on DMVPN

Example: BFD Support on DMVPN

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

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

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

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

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

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

```
interface Tunnel1
ip address 18.0.0.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp network-id 12
ip nhrp nhs 10.0.0.1 nbma 10.0.0.10 multicast
bfd template sample
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel key 18
tunnel protection ipsec profile MY_PROFILE
!
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 3
echo
!
router eigrp 2
bfd interface Tunnel1    ------------------------> Specify the interface on which the routing
 protocol must act for BFD up/down events
network 11.0.0.0 0.0.0.255
network 111.0.0.0 0.0.0.255
```

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

The following sample output shows a summary output on hub:

```
device#show dmvpn

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

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

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

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

The following sample output shows a summary output on spoke:

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

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

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

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

```
device#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel2 created 00:00:15, expire 00:04:54
   Type: dynamic, Flags: router nhop rib bfd
   NBMA address: 172.17.0.2
10.0.0.11/32 via 10.0.0.11
   Tunnel2 created 00:09:04, never expire
   Type: static, Flags: used bfd
   NBMA address: 172.17.0.11
192.168.1.0/24 via 10.0.0.1
   Tunnel2 created 00:00:05, expire 00:04:54
   Type: dynamic, Flags: router unique local
   NBMA address: 172.17.0.1
    (no-socket)
192.168.2.0/24 via 10.0.0.2
   Tunnel2 created 00:00:05, expire 00:04:54
   Type: dynamic, Flags: router rib nho
   NBMA address: 172.17.0.2
```

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

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

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

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

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

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

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

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

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

 Tunnel1:
    BFD: Disabled

 Tunnel2:
    BFD: Enabled
```

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

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 HSRP	"Configuring HSRP" module of the *Cisco IOS IP Application Services Configuration Guide*
Configuring and monitoring IS-IS	"Configuring Integrated IS-IS" 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*

Related Topic	Document Title
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*
EIGRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: Protocol-Independent Command Reference*
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*
IS-IS 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*
BFD IPv6 Encapsulation Support	"*BFD IPv6 Encapsulation Support*" module
OSPFv3 for BFD	"*OSPFv3 for BFD*" module
Static Route Support for BFD over IPv6	"*Static Route Support for BFD over IPv6*" module

Standards and RFCs

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

Technical Assistance

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

Feature Information for Bidirectional Forwarding Detection

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

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

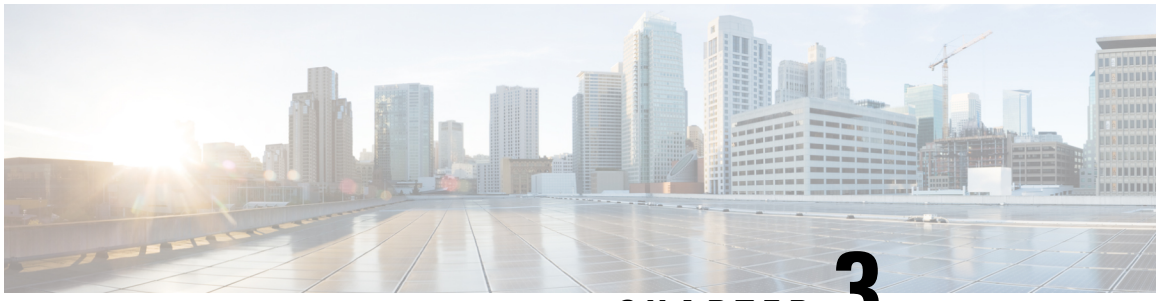
Table 1: Feature Information for Bidirectional Forwarding Detection

Feature Name	Releases	Feature Information
BFD Echo Mode	12.2(33)SRB 12.4(9)T 15.0(1)S	BFD echo mode works with asynchronous BFD. Echo packets are sent by the forwarding engine and forwarded back along the same path in order to perform detection--the BFD session at the other end does not participate in the actual forwarding of the echo packets. The echo function and the forwarding engine are responsible for the detection process, therefore the number of BFD control packets that are sent out between two BFD neighbors is reduced. And since the forwarding engine is testing the forwarding path on the remote (neighbor) system without involving the remote system, there is an opportunity to improve the interpacket delay variance, thereby achieving quicker failure detection times than when using BFD Version 0 with BFD control packets for the BFD session.
BFD IPv6 Encapsulation Support	Cisco IOS XE Release 3.11S	This feature extends IPv6 support for BFD. The following command was introduced or modified: **bfd interval**
BFD Multihop	15.1(3)S 15.4(1)S	This feature supports multihop BFD for IPv4 and IPv6 addresses. The following commands were introduced or modified: **authentication**, **bfd map**, **bfd-template**, **interval**, **show bfd neighbors**, **show bfd neighbor drops**.

Feature Name	Releases	Feature Information
BFD—Static Route Support	12.2(33)SRC 15.0(1)M 15.0(1)S 15.0(1)SY 15.1(2)S 15.1(1)SG 15.4(1)S	Unlike dynamic routing protocols, such as OSPF and BGP, static routing has no method of peer discovery. Therefore, when BFD is configured, the reachability of the gateway is completely dependent on the state of the BFD session to the specified neighbor. Unless the BFD session is up, the gateway for the static route is considered unreachable, and therefore the affected routes will not be installed in the appropriate RIB. A single BFD session can be used by an IPv4 static client to track the reachability of next hops through a specific interface. A BFD group can be assigned for a set of BFD-tracked static routes. The following commands were introduced or modified: **ip route static bfd** and **show ip static route bfd**.
BFD Support for IP Tunnel (GRE, with IP address)	15.1(1)SY	This feature supports BFD forwarding on point-to-point IPv4, IPv6, and GRE tunnels. The following commands were introduced or modified: **bfd** .
BFD Support over Port Channel	15.1(1)SY 15.1(2)SY	This feature supports configuring BFD timers on port channel interface. The following commands were introduced or modified: **bfd** .
BFD—VRF Support	12.2(33)SRC 15.0(1)M 15.0(1)S 15.1(1)SY	The BFD feature support is extended to be VPN Routing and Forwarding (VRF) aware to provide fast detection of routing protocol failures between provider edge (PE) and customer edge (CE) devices.
BFD—WAN Interface Support	12.2(33)SRC 15.0(1)M 15.0(1)S	The BFD feature is supported on nonbroadcast media interfaces including ATM, POS, serial, and VLAN interfaces. BFD support also extends to ATM, FR, POS, and serial subinterfaces. The **bfd interval** command must be configured on the interface to initiate BFD monitoring.

Feature Name	Releases	Feature Information
Bidirectional Forwarding Detection (standard implementation, Version 1)	12.0(31)S 12.0(32)S 12.2(33)SRB 12.2(33)SRC 12.2(18)SXE 12.2(33)SXH 12.4(9)T 12.4(11)T 12.4(15)T 15.0(1)S 15.4(1)S	This document describes how to enable the Bidirectional Forwarding Detection (BFD) protocol. BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.
HSRP Support for BFD	12.2(33)SRC 12.4(11)T 12.4(15)T	In Release 12.4(11)T, support for HSRP was added. In Release 12.2(33)SRC, the number of BFD sessions that can be created has been increased, BFD support has been extended to ATM, FR, POS, and serial subinterfaces, the BFD feature has been extended to be VRF-aware, BFD sessions are placed in an “Admin Down” state during a planned switchover, and BFD support has been extended to static routing.
IS-IS Support for BFD over IPv4	12.0(31)S 12.2(18)SXE 12.2(33)SRA 12.4(4)T 15.0(1)S 15.4(1)S	BFD support for OSPF can be configured globally on all interfaces or configured selectively on one or more interfaces. When BFD support is configured with IS-IS as a registered protocol with BFD, IS-IS receives forwarding path detection failure messages from BFD.
OSPF Support for BFD over IPv4	12.0(31)S 12.2(18)SXE 12.2(33)SRA 12.4(4)T 15.0(1)S 15.1(1)SG	BFD support for OSPF can be configured globally on all interfaces or configured selectively on one or more interfaces. When BFD support is configured with OSPF as a registered protocol with BFD, OSPF receives forwarding path detection failure messages from BFD.

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



CHAPTER 3

Static Route Support for BFD over IPv6

Finding Feature Information

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

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

Information About Static Route Support for BFD over IPv6

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

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

BFDv6 Associated Mode

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

An IPv6 static route requests a BFDv6 session for each static BFDv6 neighbor that has one or more associated IPv6 static routes and is configured over an interface on which BFD has been configured. The state of the

BFDv6 session will be used to determine whether the associated IPv6 static routes are inserted in the IPv6 RIB. For example, static routes are inserted in the IPv6 RIB only if the BFDv6 neighbor is reachable, and the static route is removed from the IPv6 RIB if the BFDv6 neighbor subsequently becomes unreachable.

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

BFDv6 Unassociated Mode

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

Unassociated mode is useful in the following situations:

- Bringing up a BFDv6 session in the absence of an IPv6 static route—This case occurs when a static route is on router A, with router B as the next hop. Associated mode requires you to create both a static BFD neighbor and static route on both routers in order to bring up the BFDv6 session from B to A. Specifying the static BFD neighbor in unassociated mode on router B avoids the need to configure an unwanted static route.
- Transition to BFD monitoring of a static route—This case occurs when existing IPv6 static routes are inserted in the IPv6 RIB. Here, you want to enable BFD monitoring for these static routes without any interruption to traffic. If you configure an attached IPv6 static BFD neighbor, then the static routes will immediately be associated with the new static BFD neighbor. However, because a static BFD neighbor starts in a down state, the associated static routes are then removed from the IPv6 RIB and are reinserted when the BFDv6 session comes up. Therefore, you will see an interruption in traffic. This interruption can be avoided by configuring the static BFD neighbor as unassociated, waiting until the BFDv6 session has come up, and then reconfiguring the static BFD neighbor as associated.
- Transition from BFD monitoring of a static route—In this case, IPv6 static routes are monitored by BFD and inserted in the RIB. Here, you want to disable BFD monitoring of the static routes without interrupting traffic flow. This scenario can be achieved by first reconfiguring the static BFD neighbor as detached (thus disassociating the neighbor from the static routes) and then deconfiguring the static BFD neighbor.

How to Configure Bidirectional Forwarding Detection for IPv6

Specifying a Static BFDv6 Neighbor

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**] **Example:** `Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1`	Specifies static route IPv6 BFDv6 neighbors.

Associating an IPv6 Static Route with a BFDv6 Neighbor

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]
4. **ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix / prefix-length* {*ipv6-address* | *interface-type interface-number ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*]

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**] **Example:** `Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1`	Specifies static route BFDv6 neighbors.
Step 4	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix / prefix-length* {*ipv6-address* | *interface-type interface-number ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **Example:** `Device(config)# ipv6 route 2001:DB8::/64 gigabitethernet 0/0/0 2001::1`	Establishes static IPv6 routes.

Configuration Examples for Static Route Support for BFD over IPv6

Example: Specifying an IPv6 Static BFDv6 Neighbor

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

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

Example: Associating an IPv6 Static Route with a BFDv6 Neighbor

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

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

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
Static Route Support for BFD over IPv6	" *Bidirectional Forwarding Detection*" module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

Technical Assistance

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

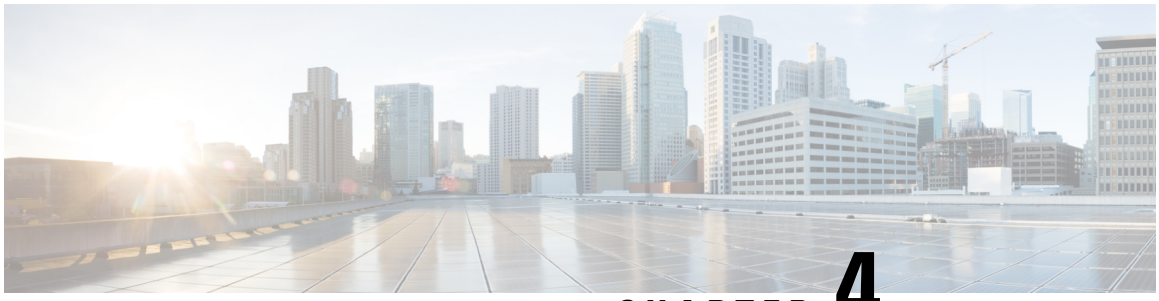
Feature Information for Static Route Support for BFD over IPv6

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

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

Table 2: Feature Information for Static Route Support for BFD over IPv6

Feature Name	Releases	Feature Information
Static Route Support for BFD over IPv6	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.6S	Using the BFDv6 protocol to reach the static route next hop ensures that an IPv6 static route is inserted only in the IPv6 Routing Information Base (RIB) when the next-hop neighbor is reachable. Using the BFDv6 protocol also can remove the IPv6 static route from the IPv6 RIB when the next hop becomes unreachable. The following commands were introduced or modified: **debug bfd**, **debug ipv6 static**, **ipv6 static**, **ipv6 route static bfd**, **monitor event ipv6 static**, **show ipv6 static**.



CHAPTER 4

OSPFv3 for BFD

The Bidirectional Forwarding Detection protocol supports OSPFv3.

Finding Feature Information

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

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

Information About OSPFv3 for BFD

The Bidirectional Forwarding Detection (BFD) protocol supports Open Shortest Path First version 3 (OSPFv3).

How to Configure OSPFv3 for BFD

Configuring BFD Support for OSPFv3

This section describes the procedures for configuring BFD support for OSPFv3, so that OSPFv3 is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD. You can either configure BFD support for OSPFv3 globally on all interfaces or configure it selectively on one or more interfaces.

There are two methods for enabling BFD support for OSPFv3:

- You can enable BFD for all of the interfaces for which OSPFv3 is routing by using the **bfd all-interfaces** command in router configuration mode. You can disable BFD support on individual interfaces using the **ipv6 ospf bfd disable** command in interface configuration mode.
- You can enable BFD for a subset of the interfaces for which OSPFv3 is routing by using the **ipv6 ospf bfd** command in interface configuration mode.

Note OSPF will only initiate BFD sessions for OSPF neighbors that are in the FULL state.

Configuring Baseline BFD Session Parameters on the Interface

Repeat this task for each interface over which you want to run BFD sessions to BFD neighbors.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** `Device(config-if)# bfd interval 50 min_rx 50 multiplier 5`	Enables BFD on the interface.

Configuring BFD Support for OSPFv3 for All Interfaces

Before you begin

OSPFv3 must be running on all participating devices. The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id* [**vrf** *vpn-name*]
4. **bfd all-interfaces** [**strict-mode**]
5. **exit**
6. **show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6** *ipv6-address*] [**details**]
7. **show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# ipv6 router ospf 2`	Configures an OSPFv3 routing process.
Step 4	**bfd all-interfaces** [**strict-mode**] **Example:** `Device(config-router)# bfd all-interfaces`	Enables BFD for all interfaces participating in the routing process. **[strict-mode]** - BFD session is established in the strict-mode. In the strict-mode, the OSPF session is not established till the BFD session is established.
Step 5	**exit** **Example:** `Device(config-router)# exit`	Enter this command twice to go to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6** *ipv6-address*] [**details**] **Example:** `Device# show bfd neighbors detail`	(Optional) Displays a line-by-line listing of existing BFD adjacencies.
Step 7	**show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**] **Example:** `Device# show ipv6 ospf`	(Optional) Displays general information about OSPFv3 routing processes. If BFD is enabled in strict-mode, the command output displays `BFD is enabled in strict mode`.

Configuring BFDv6 Support for OSPFv3 on One or More OSPFv3 Interfaces

Before you begin

OSPFv3 must be running on all participating devices. The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf bfd** [**disable**] [**strict-mode**]
5. **exit**
6. **show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address*| **ipv6** *ipv6-address*] [**details**]
7. **show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Specifies an interface type and number, and places the device in interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface GigabitEthernet 0/0/0`	
Step 4	**ipv6 ospf bfd** [**disable**] [**strict-mode**] **Example:** `Device(config-if)# ipv6 ospf bfd`	Enables BFD on a per-interface basis for one or more interfaces associated with the OSPFv3 routing process. **[strict-mode]** - BFD session is established in the strict-mode. In the strict-mode, the OSPF session is not established till the BFD session is established.
Step 5	**exit** **Example:** `Device(config-router)# exit`	Enter this command twice to go to privileged EXEC mode.
Step 6	**show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address*| **ipv6** *ipv6-address*] [**details**] **Example:** `Device# show bfd neighbors detail`	(Optional) Displays a line-by-line listing of existing BFD adjacencies.
Step 7	**show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**] **Example:** `Device# show ipv6 ospf`	(Optional) Displays general information about OSPFv3 routing processes. If BFD is enabled in strict-mode, the command output displays `BFD is enabled in strict mode`.

Retrieving BFDv6 Information for Monitoring and Troubleshooting

SUMMARY STEPS

1. **enable**
2. **monitor event ipv6 static** [**enable** | **disable**]
3. **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface** *type number* | **recursive**] [**vrf** *vrf-name*] [**bfd**] [**detail**
4. **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface** *type number* | **recursive**] [**vrf** *vrf-name*] [**bfd**] [**detail**]
5. **debug ipv6 static**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**monitor event ipv6 static** [**enable** | **disable**] **Example:** `Device# monitor event ipv6 static enable`	Enables the use of event trace to monitor the operation of the IPv6 static and IPv6 static BFDv6 neighbors.
Step 3	**show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface** *type number* | **recursive**] [**vrf** *vrf-name*] [**bfd**] [**detail** **Example:** `Device# show ipv6 static vrf vrf1 detail`	Displays the BFDv6 status for a static route associated with a static BFDv6 neighbor.
Step 4	**show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface** *type number* | **recursive**] [**vrf** *vrf-name*] [**bfd**] [**detail**] **Example:** `Device# show ipv6 static vrf vrf1 bfd`	Displays static BFDv6 neighbors and associated static routes.
Step 5	**debug ipv6 static** **Example:** `Device# debug ipv6 static`	Enables BFDv6 debugging.

Configuration Examples for OSPFv3 for BFD

Example: Displaying OSPF Interface Information about BFD

The following display shows that the OSPF interface is enabled for BFD:

```
Device# show ipv6 ospf interface

Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/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 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*
OSPFv3 for BFD	"*Bidirectional Forwarding Detection*" module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

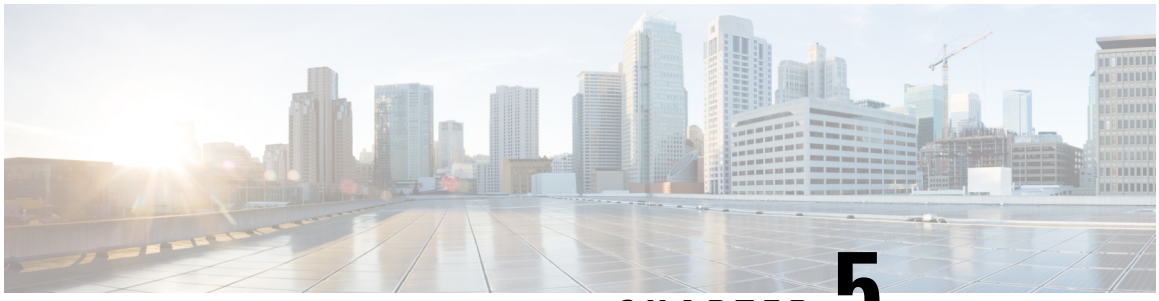
Feature Information for OSPFv3 for BFD

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

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

Table 3: Feature Information for OSPFv3 for BFD

Feature Name	Releases	Feature Information
OSPFv3 for BFD	Cisco IOS XE Release 2.1	BFD supports the dynamic routing protocol OSPFv3. The following commands were introduced or modified: **bfd**, **bfd all-interfaces**, **debug bfd**, **ipv6 router ospf**, **show bfd neighbors**, **show ipv6 ospf**, **show ipv6 ospf interface**, **show ospfv3**, **show ospfv3 interface**.



CHAPTER 5

BFD on BDI Interfaces

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

Finding Feature Information

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

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

Information About BFD on Bridge Domain Interfaces

BFD on Bridge Domain Interfaces

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

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

How to Configure BFD on BDI Interfaces

Enabling BFD on a Bridge Domain Interface

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

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

Before you begin

Two or more nodes must be connected.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface bdi 100`	Configures a bridge domain interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.201.201.1 255.255.255.0`	Configures an IP address for the interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Associating an Ethernet Flow Point with a Bridge Domain

Before you begin

BFD must be enabled on both nodes.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/subslot/port* **Example:** `Router(config)# interface GigabitEthernet0/0/3`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables IP processing.
Step 5	**negotiation auto** **Example:** `Router(config-if)# negotiation auto`	Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the interface.
Step 6	**cdp enable** **Example:** `Router(config-if)# cdp enable`	Enables Cisco Discovery Protocol on the interface.
Step 7	**service instance** *id service-type* **Example:** `Router(config-if)# service instance 2 ethernet`	Configures an Ethernet service instance and enters service instance configuration mode.
Step 8	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 2`	Enables IEEE 802.1Q encapsulation of traffic on the subinterface.
Step 9	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies removal of the outermost tag from the frame ingressing the service instance and the addition of a tag in the egress direction.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits service instance configuration mode and returns to interface configuration mode.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 12	**bridge-domain** *vlan-id* **Example:** `Router(config)# bridge-domain 2`	Associates the bridge domain with the Ethernet flow point.

Example:

What to do next

Configuration Examples for BFD on BDI Interfaces

Examples for BFD on BDI Interfaces

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

```
Router#show bfd neighbors

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
10.1.1.2                              2049/1         Up        Up        BD2
Router#
Router#show running interface gi0/0/3
Building configuration...

Current configuration : 230 bytes
!
interface GigabitEthernet0/0/3
no ip address
ip pim passive
ip igmp version 3
negotiation auto
cdp enable
service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
!
end

Router#show running interface bdi2

Building configuration...

Current configuration : 127 bytes
!
interface BDI2
ip address 10.1.1.3 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3
bfd neighbor ipv4 10.1.1.2
end
```

And similarly for the other node:

```
Router2#show running interface bdi2
```

```
Building configuration...

Current configuration : 127 bytes
!
interface BDI2
ip address 10.1.1.2 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3
bfd neighbor ipv4 10.1.1.3
end

ED3#show run int gig0/0/3
Building configuration...

Current configuration : 195 bytes
!
interface GigabitEthernet0/0/3
no ip address
negotiation auto
cdp enable
service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
!
end

Router2#show bfd neighbors

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
10.1.1.3                                1/2049       Up        Up        BD2
ED3#
```

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 HSRP	"Configuring HSRP" module of the *Cisco IOS IP Application Services Configuration Guide*
Configuring and monitoring IS-IS	"Configuring Integrated IS-IS" module of the *Cisco IOS IP Routing Protocols Configuration Guide*

Related Topic	Document Title
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*
EIGRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: Protocol-Independent Command Reference*
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*
IS-IS 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*
BFD IPv6 Encapsulation Support	"*BFD IPv6 Encapsulation Support*" module
OSPFv3 for BFD	"*OSPFv3 for BFD*" module
Static Route Support for BFD over IPv6	"*Static Route Support for BFD over IPv6*" module

Standards and RFCs

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

Technical Assistance

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

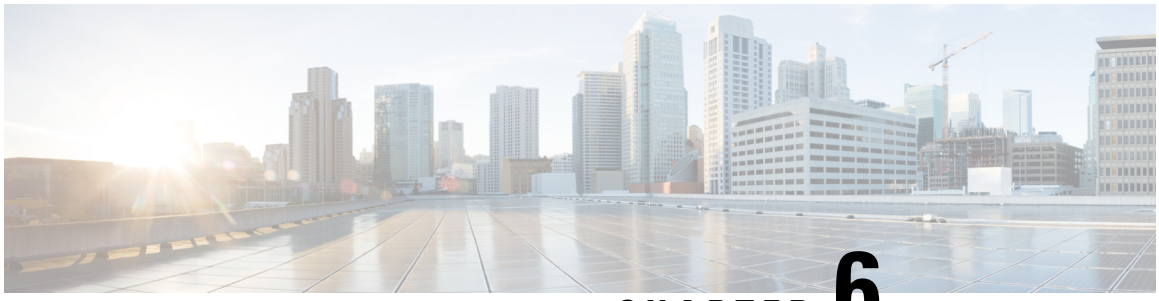
Feature Information for BFD on Bridge Domain Interfaces

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

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

Table 4: Feature Information for BFD on Bridge Domain Interfaces

Feature Name	Releases	Feature Information
BFD on Bridge Domain Interfaces	Cisco IOS XE Release 3.5S	This feature supports BFD on Bridge Domain Interfaces.



CHAPTER 6

BFD Single-Hop Authentication

The BFD Single-Hop Authentication feature enables authentication for single-hop Bidirectional Forwarding Detection (BFD) sessions between two directly connected devices. This feature supports Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) authentication types.

This module explains the BFD Single-Hop Authentication feature.

Finding Feature Information

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

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

Prerequisites for BFD Single-Hop Authentication

You must configure keys and key chains on both connected devices that are involved in a BFD session. You must configure the algorithm and the key chain on both devices in such a way that the configurations match.

Restrictions for BFD Single-Hop Authentication

- If key chains are removed from the established BFD single-hop sessions or no active keys are present in the key chain, the BFD template and the map entry are invalidated. Such invalidation is considered as a map entry deletion.
- Meticulous keyed MD5 authentication and meticulous keyed SHA-1 are not supported in In-Service Software Upgrade (ISSU) because checkpointing of sequence numbers does not occur in all packets.
- Meticulous MD5 and meticulous SHA-1 authentication types are not preserved after Route Processor (RP) failures in Stateful Switchover (SSO) mode. The sessions could flap causing link instability of the registered protocols.
- Only timers with values greater than or equal to 50 milliseconds are supported.
- The authentication type negotiation and key exchange between two BFD peers does not occur.
- When there is a missing key chain or when keys are not configured in a key chain, the BFD template and its associated map entries are invalidated, and the BFD session is not created.
- You can apply Bidirectional Forwarding Detection (BFD) single-hop Authentication in a BFD-template configuration only. You cannot apply BFD single-hop authentication in legacy configurations.

Information About BFD Single-Hop Authentication

Benefits of BFD Single-Hop Authentication

Using the Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) authentication methods defined in RFC 5880, the BFD Single Hop Authentication feature provides security against attacks on data links between a pair of directly connected devices involved in a BFD session. This feature is applied on data links between a BFD source-destination pair that communicates through IPv4 and IPv6 protocols across a single IP hop that is associated with an incoming interface. The communication may occur through physical media, virtual circuits, and tunnels.

Role of BFD Single-Hop Authentication in Preventing Denial of Service Attacks

To prevent denial of service (DoS) attacks, a BFD single-hop session validates the sequence number of a packet on receiving the packet. Detect multiplier is the number of missing BFD hello messages from another BFD device before the local device detects a fault in the forwarding path. The detect multiplier is used to determine the detect timer. The following are the ranges of valid sequence numbers that are accepted by the BFD Single-Hop Authentication feature:

- For nonmeticulous keyed types: Last received sequence number to (last received sequence number + 3 * detect multiplier)
- For meticulous keyed types: Last received sequence number + 1) to (last received sequence number + 3 * detect multiplier)

Note For BFD, (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.

How to Configure BFD Single-Hop Authentication

Configuring Key Chains

Perform this task on one of the two devices that are involved in a BFD session, and repeat the steps on the other device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *chain-name*
4. **key** *key-id*
5. **key-string** *text*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *chain-name* **Example:** `Device(config)# key chain chain1`	Defines an authentication key chain needed to enable authentication for routing protocols and enters key-chain configuration mode.
Step 4	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Defines an authentication key on the key chain and enters keychain-key configuration mode.
Step 5	**key-string** *text* **Example:** `Device(config-keychain-key)# key-string key1`	Defines an authentication string for a key.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-keychain-key)# end`	Exits keychain-key configuration mode and returns to privileged EXEC mode.

Configuring a BFD Template with Authentication

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**bfd-template single-hop** *template-name* **Example:** `Device(config)# bfd-template single-hop template1`	Creates a BFD template and enters BFD configuration mode.
Step 4	**interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value* **Example:** `Device(config-bfd)# interval min-tx 120 min-rx 100 multiplier 3`	Configures transmit and receive intervals between BFD packets and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.
Step 5	**authentication** *authentication-type* **keychain** *keychain-name* **Example:** `Device(config-bfd)# authentication sha-1 keychain keychain1`	Configures authentication in a BFD template for single-hop sessions.
Step 6	**end** **Example:**	Exits BFD configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-bfd)# end`	

Configuring a Single-Hop Template on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd template** *template-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/1`	Enters interface configuration mode.
Step 4	**bfd template** *template-name* **Example:** `Device(config-if)# bfd template bfdtemplate`	Binds a single-hop BFD template to an interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying BFD Single-Hop Authentication

SUMMARY STEPS

1. **show bfd drops**
2. **show bfd neighbor**

DETAILED STEPS

Step 1 **show bfd drops**

Example:

```
Device> show bfd drops
```

This command displays the number of dropped packets in BFD.

Step 2 **show bfd neighbor**

Example:

```
Device> show bfd neighbor
```

This command displays a line-by-line listing of existing BFD adjacencies.

Configuration Examples for BFD Single-Hop Authentication

Example: Configuring Key Chains

```
Device> enable
Device# configure terminal
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# end
```

Example: Configuring a BFD Template with Authentication

```
Device> enable
Device# configure terminal
Device(config)# bfd-template single-hop template1
Device(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
Device(bfd-config)# authentication sha-1 keychain keychain1
Device(bfd-config)# end
```

Example: Configuring a Single-Hop Template on an Interface

```
Device> enable
Device# configure terminal
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# end
```

Example: Verifying BFD Single-Hop Authentication

Sample Output for the show bfd neighbor command

```
Device> show bfd neighbor

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.168.0.2                            1/12          Up        Up        Et0/0
Session state is UP and using echo function with 300 ms interval.
Session Host: Software
OurAddr: 192.168.0.1
Handle: 12
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(62244)
Rx Count: 62284, Rx Interval (ms) min/max/avg: 1/2436/878 last: 239 ms ago
Tx Count: 62247, Tx Interval (ms) min/max/avg: 1/1545/880 last: 246 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub CEF
Template: my-template
Authentication(Type/Keychain): sha-1/my-chain
Uptime: 00:22:06
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 12             - Your Discr.: 1
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 300000
```

Sample Output for the show bfd drops command.

```
Device> show bfd drops

BFD Drop Statistics
                        IPV4    IPV6    IPV4-M  IPV6-M  MPLS_PW MPLS_TP_LSP
Invalid TTL             0       0       0       0       0       0
BFD Not Configured      0       0       0       0       0       0
No BFD Adjacency        0       0       0       0       0       0
Invalid Header Bits     0       0       0       0       0       0
Invalid Discriminator   0       0       0       0       0       0
Session AdminDown       0       0       0       0       0       0
Authen invalid BFD ver  0       0       0       0       0       0
Authen invalid len      0       0       0       0       0       0
Authen invalid seq      0       0       0       0       0       0
Authen failed           0       0       0       0       0       0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
IP Routing: Protocol-Independent Commands	*Cisco IOS IP Routing Protocol-Independent Command Reference*

Standards and RFCs

Standard/RFC	Title
RFC 5880	*Bidirectional Forwarding Detection*

Technical Assistance

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

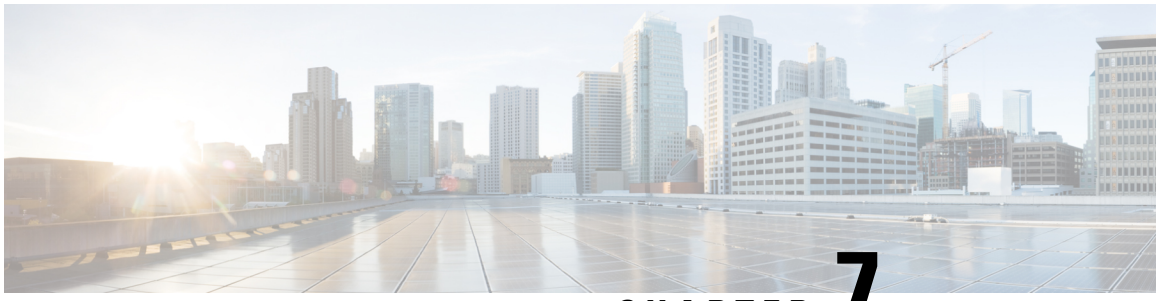
Feature Information for BFD Single-Hop Authentication

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

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

Table 5: Feature Information for BFD Single Hop Authentication

Feature Name	Releases	Feature Information
BFD Single-Hop Authentication	15.2(4)S	The BFD Single-Hop Authentication feature enables authentication for single hop BFD sessions between directly connected devices. This feature supports Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1) authentication types. The following commands were introduced or modified: **authentication (BFD)**, **bfd template**, **bfd-template**, **show bfd drops** and **show bfd neighbors**.



CHAPTER 7

BFD Multihop Support for IPv4 Static Routes

The BFD Multihop Support for IPv4 Static Routes feature enables detection of IPv4 network failure between paths that are not directly connected. If a Bidirectional Forwarding Detection (BFD) session is up (that is, the next-hop destination is reachable), IPv4 static routes that are associated with IPv4 static BFD configuration are added to a routing table. If the BFD session is down, the routing table removes all associated static routes from the routing table.

This feature is applicable on different kinds of interfaces such as physical, subinterface, and virtual tunnels and across intra-area and interarea topologies.

Finding Feature Information

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

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

Prerequisites for BFD Multihop Support for IPv4 Static Routes

- The BFD destination for which an IPv4 static route has to be configured must be reachable by all devices.
- The configured device must have at least one static route with the next-hop destination as a BFD destination for an associated session. If not, the BFD session is not created on the device.

Information About BFD Multihop Support for IPv4 Static Routes

BFDv4 Associated Mode

In Bidirectional Forwarding Detection for IPv4 (BFDv4) associated mode, an IPv4 static route is automatically associated with an IPv4 static BFDv4 multihop destination address if the static route next hop exactly matches the static BFDv4 multihop destination address.

The state of the BFDv4 session is used to determine whether the associated IPv4 static routes are added in the IPv4 routing information base (RIB). For example, static routes are added in the IPv4 RIB only if the BFDv4 multihop destination is reachable, and the static routes are removed from the IPv4 RIB if the BFDv4 multihop destination subsequently becomes unreachable.

BFDv4 Unassociated Mode

In Bidirectional Forwarding Detection for IPv4 (BFDv4), an IPv4 static BFD multihop destination can be configured in unassociated mode. In unassociate mode, a BFD neighbor is not associated with a static route, and the BFD sessions are requested if the IPv4 static BFD is configured.

Unassociated mode is useful in the following scenario:

- Absence of an IPv4 static route—This scenario occurs when a static route is on device A, and device B is the next hop. In associated mode, you must create both a static BFD multihop destination address and a static route on both devices to bring up the BFDv4 session from device B to device A. Specifying the static BFD multihop destination in unassociated mode on device B avoids the need to configure an unwanted static route.

How to Configure BFD Multihop Support for IPv4 Static Routes

Configuring BFD Multihop IPv4 Static Routes

Before you begin

- Specify a BFD destination address which is same as the IPv4 static route next hop or gateway address.
- Configure a BFD map and a BFD multihop template for an interface on the device. The destination address and source address configured for a BFD map must match the BFD static multihop configuration and the source address must be a valid IP address configured for an interface in the routing table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask ip-address*
4. **ip route static bfd** *multihop-destination-address multihop-source-address*
5. **ip route static bfd** *multihop-destination-address multihop-source-address* **unassociate**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip route** *prefix mask ip-address* **Example:** `Device(config)# ip route 192.0.2.0 255.255.255.0 10.1.1.2`	Configures an IPv4 static route that BFD multihop uses to monitor static routes.
Step 4	**ip route static bfd** *multihop-destination-address multihop-source-address* **Example:** `Device(config)# ip route static bfd 192.0.2.1 10.1.1.1`	Configures the static IPv4 BFD multihop to be associated with a static IPv4 route.
Step 5	**ip route static bfd** *multihop-destination-address multihop-source-address* **unassociate** **Example:** `Device(config)# ip route static bfd 192.0.2.1 10.1.1.1 unassociate`	(Optional) Configures the static IPv4 BFD multihop to be associated with a static IPv4 route in unassociated mode.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying BFD Multihop Support for IPv4 Static Routes

The following show commands can be used to verify IPv4 static routes for BFD multihop:

SUMMARY STEPS

1. **show bfd neighbor**
2. **show ip static route bfd**

DETAILED STEPS

Step 1 **show bfd neighbor**

Displays a line-by-line listing of existing BFD adjacencies.

Step 2 **show ip static route bfd**

Displays information about the IPv4 static BFD configured parameters.

Configuration Examples for BFD Multihop Support for IPv4 Static Routes

Example: Configuring BFD Multihop for IPv4 Static Routes in Associated Mode

```
Device> enable
Device# configure terminal
Device(config)# bfd map ipv4 192.0.2.1/32  10.1.1.1/32 test
Device(config)# bfd-template multi-hop test
Device(config-bfd)# interval min-tx 51 min-rx 51 multiplier 3
Device(config-bfd)# exit
Device(config)# ip route 192.0.2.0 255.255.255.0 10.1.1.2
Device(config)# interface GigabitEthernet 1/1
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# exit
Device(config)# ip route static bfd 192.0.2.1 10.1.1.1
Device(config)# end
```

Example: Configuring IPv4 Static Multihop for BFD in Unassociated Mode

```
Device> enable
Device# configure terminal
Device(config)# bfd map ipv4 192.0.2.1/32  10.1.1.1/32 test
Device(config)# bfd-template multi-hop test
Device(config-bfd)# interval min-tx 51 min-rx 51 multiplier 3
Device(config-bfd)# exit
Device(config)# ip route 192.0.2.0 255.255.255.0 10.1.1.2
Device(config)# interface GigabitEthernet 1/1
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# exit
Device(config)# ip route static bfd 192.0.2.1 10.1.1.1 unassociate
Device(config)# end
```

Additional References for BFD Multihop Support for IPv4 Static Routes

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
IP Routing: Protocol Independent commands	*IP Routing Protocol-Independent Command Reference*

Standards and RFCs

Standard/RFC	Title
RFC 5883	*BFD for Multihop Paths*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

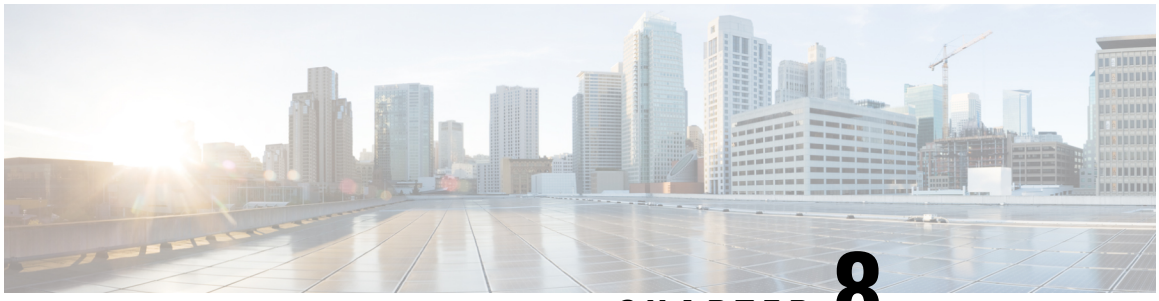
Feature Information for BFD Multihop Support for IPv4 Static Routes

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

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

Table 6: Feature Information for BFD Multihop Support for IPv4 Static Routes

Feature Name	Releases	Feature Information
BFD Multihop Support for IPv4 Static Routes	Cisco IOS XE Release 3.9S	The BFD Multihop Support for IPv4 Static Routes feature enables detection of IPv4 network failure between paths that are not directly connected. If a Bidirectional Forwarding Detection (BFD) session is up (that is, the next-hop destination is reachable), IPv4 static routes that are associated with IPv4 static BFD configuration are added to a routing table. If the BFD session is down, the routing table removes all associated static routes from the routing table. The following commands were modified: **ip route static bfd** and **show ip static route bfd**.



CHAPTER 8

IS-IS IPv6 Client for BFD

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

Finding Feature Information

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

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

Prerequisites for IS-IS IPv6 Client for BFD

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

Information About IS-IS IPv6 Client for BFD

IS-IS BFD Topology

When BFD support is configured with IS-IS as a registered protocol with BFD, IS-IS receives forwarding path detection failure messages from BFD. BFD support for IS-IS can be configured in either router address-family configuration mode or interface configuration mode. IS-IS IPv6 can run in single-topology or in Multi-Topology (MT) mode.

IS-IS BFD supports both IPv4 and IPv6 on the same adjacency for single-topology or multi-topology mode. If BFD is enabled for both IPv4 and IPv6, IS-IS sends two BFD session creation requests to BFD. For single-topology mode, the IS-IS adjacency state can only be UP if both BFD sessions are UP. If either of the BFD sessions is DOWN, the associated IS-IS adjacency state is also DOWN. For MT mode, the IS-IS adjacency state can be UP as long as one of topologies has a BFD session in an UP state.

IS-IS BFD IPv6 Session Creation

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

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

IS-IS BFD IPv6 Session Deletion

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

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

How to Configure ISIS IPv6 Client for BFD

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *ipv6-address/mask*
5. **isis ipv6 bfd**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 6/0/0`	Enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address/mask* **Example:** `Device(config-if)# ipv6 address 19:1:1::4/64`	Configures IPv6.
Step 5	**isis ipv6 bfd** **Example:** `Device(config-if)# isis ipv6 bfd`	Enables IPv6 BFD on a specific interface that is configured for IS-IS.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Device(config)# router isis`	Enables the IS-IS routing protocol and enters router configuration mode.
Step 4	**metric-style wide** **Example:** `Device(config-router)# metric-style wide`	(Optional) Configures a device that is running IS-IS so that it generates and accepts only new-style type, length, value objects (TLVs).
Step 5	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enters address family configuration mode for configuring IS-IS routing sessions that use standard IPv6 address prefixes.
Step 6	**multi-topology** **Example:** `Device(config-router-af)# multi-topology`	(Optional) Enables multi-topology IS-IS for IPv6.

	Command or Action	Purpose
Step 7	**bfd all-interfaces** **Example:** `Device(config-router-af)# bfd all-interfaces`	Enables BFD for all interfaces participating in the routing process.
Step 8	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Configuration Examples for ISIS IPv6 Client for BFD

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

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 6/0/0
Device(config-if)# ipv6 address 19:111:112::2/64
Device(config-if)# isis ipv6 bfd
Device(config-if)# end
```

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 6/0
Device(config-if)# ipv6 address 19:111:112::1/64
Device(config-if)# isis ipv6 bfd
Device(config-if)# end
```

Example: IS-IS IPv6 Client Support for BFD on All Interfaces

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# metric-style wide
Device(config-router)# address-family ipv6
Device(config-router-af)# multi-topology
Device(config-router-af)# bfd all-interfaces
Device(config-router-af)# end
```

The following is a sample configuration where interface 0/0/7 of Router A is connected to interface 0/4/6 of router B.

Configuration for Router A

```
bfd-template single-hop BFDM
 interval min-tx 50 min-rx 50 multiplier 3
```

```
!
interface TenGigabitEthernet0/0/7
 ipv6 address 19:1:1::1/64
 ipv6 router isis
 bfd template BFDM
 isis ipv6 bfd
!
router isis
 net 49.0001.1720.1600.1001.00
!
```

Configuration on Router B

```
Router B

bfd-template single-hop BFDM
 interval min-tx 50 min-rx 50 multiplier 3
!
interface TenGigabitEthernet0/4/6
 ipv6 address 19:1:1::2/64
 ipv6 router isis
 bfd template BFDM
 isis ipv6 bfd
!
router isis
 net 49.0000.0000.0002.00
!
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
BFD commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Routing: Protocol-Independent Command Reference*
Configuring and monitoring IS-IS	"Configuring Integrated IS-IS" module of the *IP Routing Protocols Configuration Guide*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*
IPv6 commands	*Cisco IOS IPv6 Command Reference*

Technical Assistance

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

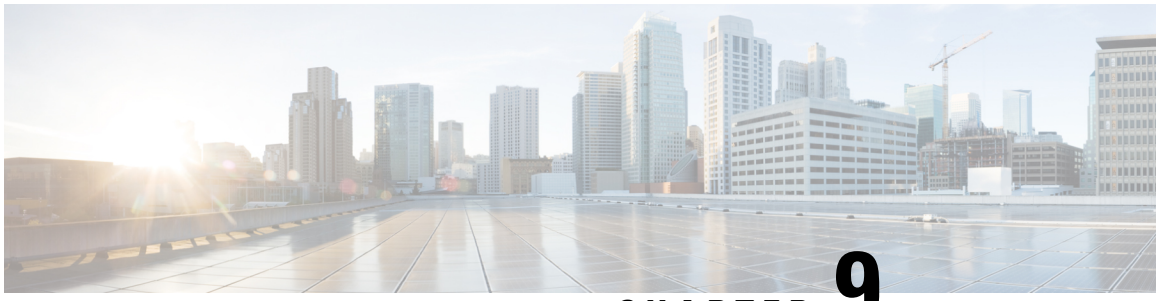
Feature Information for IS-IS IPv6 Client for BFD

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

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

Table 7: Feature Information for IS-IS IPv6 Client for BFD

Feature Name	Releases	Feature Information
IS-IS IPv6 Client for BFD	15.1(1)SY 15.2(4)S 15.3(1)T	When BFD support is configured with IS-IS as a registered protocol with BFD, IS-IS receives forwarding path detection failure messages from BFD. The following commands were introduced or modified: **bfd all-interfaces**, **isis ipv6 bfd**.



CHAPTER 9

IS-IS Client for BFD C-Bit Support

The Bidirectional Forwarding Detection (BFD) protocol provides short-duration detection of failures in the path between adjacent forwarding engines while maintaining low networking overheads. The BFD IS-IS Client Support feature enables Intermediate System-to-Intermediate System (IS-IS) to use Bidirectional Forwarding Detection (BFD) support, which improves IS-IS convergence as BFD detection and failure times are faster than IS-IS convergence times in most network topologies. The IS-IS Client for BFD C-Bit Support feature enables the network to identify whether a BFD session failure is genuine or is the result of a control plane failure due to a router restart. When planning a router restart, you should configure this feature on all neighboring routers.

Finding Feature Information

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

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

Prerequisites for IS-IS Client for BFD C-Bit Support

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

Information About IS-IS Client for BFD C-Bit Support

IS-IS Restarts and BFD Sessions

The IS-IS Client for BFD C-Bit Support feature provides BFD with a way to signal to its peers whether the BFD implementation shares the same status as the control plane. When a neighboring router's control plane restarts, a BFD session failure may occur, which does not actually represent a true forwarding failure. If this happens, you do not want the neighbors of the restarting router to react to the BFD session failure.

IS-IS does not have protocol extensions that allow it to signal in advance that it will be restarting. This means that the system cannot distinguish between a real forwarding failure and a restart. The IS-IS Client for BFD C-Bit Support feature allows you to configure the device to ignore control-plane related BFD session failures. We recommend that you configure this feature on the neighbors of a restarting device just prior to the planned restart of that device and that you remove the configuration after the restart has been completed.

The table below shows how the control plane independent failure status received from BFD on a session down event impacts IS-IS handling of that event.

Table 8: Control Plane Failure and Session Down Events

IS-IS Check Control Plane Failure	BFD Control Plane Independent Failure Status	IS-IS Action on BFD session 'DOWN' Event
Enabled	True	Accept session DOWN
Enabled	False	Ignore session DOWN
Disabled	True	Accept session DOWN
Disabled	False	Accept session DOWN

How to Configure IS-IS Client for BFD C-Bit Support

Configuring IS-IS Client for BFD C-Bit Support

Perfrom this task to enable control plane failure checking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **bfd check-control-plane-failure**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Device(config)# router isis`	Enables the IS-IS routing protocol and enters router configuration mode.
Step 4	**bfd check-control-plane-failure** **Example:** `Device(config-router)# bfd check-control-plane-failure`	Enables BFD control plane failure checking for the IS-IS routing protocol.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuration Examples for IS-IS Client for BFD C-Bit Support

Example: Configuring IS-IS Client for BFD C-Bit Support

The following example configures control plane failure detection on a router running the IS-IS protocol.

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# bfd check-ctrl-plane-failure
Device(config-router)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
BFD commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: Protocol-Independent Command Reference*
Configuring and monitoring IS-IS	"Configuring Integrated IS-IS" module of the *Cisco IOS IP Routing Protocols Configuration Guide*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFC 5882	*Generic Application of Bidirectional Forwarding Detection (BFD)*

Technical Assistance

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

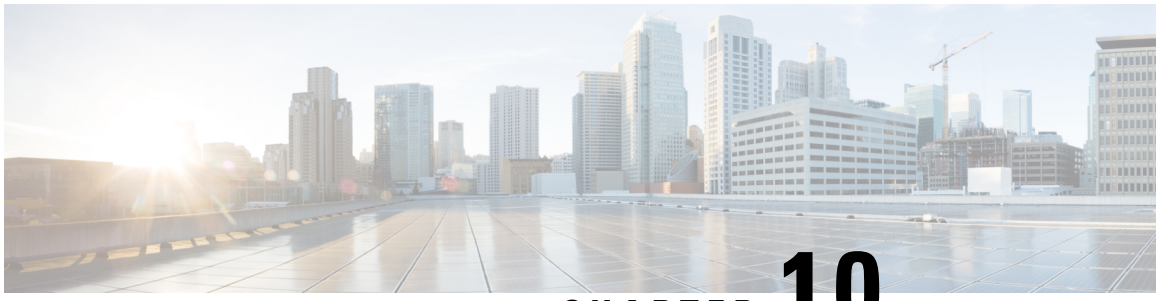
Feature Information for IS-IS Client for BFD C-Bit Support

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

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

Table 9: Feature Information for IS-IS Client for BFD C-Bit Support

Feature Name	Releases	Feature Information
IS-IS Client for BFD C-Bit Support	15.1(1)SY 15.3(1)T	The IS-IS Client for BFD C-Bit Support feature enables the network to identify whether a BFD session failure is genuine or is the result of a control plane failure due to a router restart. The following command was introduced: **bfd check-ctrl-plane-failure**.



CHAPTER 10

BFD Dampening

The BFD Dampening feature introduces a configurable exponential delay mechanism to suppress the excessive effect of remote node reachability events flapping with Bidirectional Forwarding Detection (BFD). The BFD Dampening feature allows the network operator to automatically dampen a given BFD session to prevent excessive notification to the BFD clients, thus preventing unnecessary instability in the network. Configuring the BFD Dampening feature on a high-speed interface with routing clients improves the convergence time and stability throughout the network.

Finding Feature Information

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

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

Information About BFD Dampening

Overview of BFD Dampening

Bidirectional Forwarding Detection (BFD) is a mechanism used by the routing protocols to quickly realize the reachability failures to their neighbors. When BFD detects a reachability status change of a neighbor, clients are notified immediately. Sometimes it might be critical to minimize changes in routing tables so as not to impact convergence, in case of any micro failure. An unstable link that flaps excessively can cause other devices in the network to consume substantial system processing resources, and it can cause routing protocols to lose synchronization with the state of the flapping link.

The BFD Dampening feature introduces a configurable exponential delay mechanism to suppress the excessive effect of remote node reachability events flapping with BFD. The BFD Dampening feature allows the network operator to automatically dampen a given BFD session to prevent excessive notification to the BFD clients, thus preventing unnecessary instability in the network. Dampening the notification to a BFD client suppresses BFD notification until the session under monitoring stops flapping and becomes stable.

Configuring the BFD Dampening feature, especially on a high-speed interface with routing clients, improves the convergence time and stability throughout the network. BFD dampening can be applied to all types of BFD sessions, including IPv4/single-hop/multihop, Multiprotocol Label Switching-Transport Profile (MPLS-TP), and Pseudo Wire (PW) Virtual Circuit Connection Verification (VCCV).

You can configure the BFD Dampening feature at the BFD template level (both single-hop and multihop templates). Dampening is applied to all the sessions that use the BFD template. If you do not want a session to be dampened, you should use a new BFD template without dampening for the new session. By default, the dampening functionality is not enabled on a template.

How to Configure BFD Dampening

Configuring BFD Dampening

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bfd-template multi-hop** *template-name*
4. **interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value*
5. **dampening** [*half-life-period reuse-threshold suppress-threshold max-suppress-time*]
6. **end**
7. **show bfd neighbors details**
8. **show bfd neighbors dampening**
9. **show bfd neighbors dampened**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**bfd-template multi-hop** *template-name* **Example:**	Creates a Bidirectional Forwarding Detection (BFD) template and enters BFD configuration mode.

	Command or Action	Purpose
	`Device(config)# bfd-template multi-hop doctemplate`	
Step 4	**interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value* **Example:** `Device(config-bfd)# interval min-tx 120 min-rx 100 multiplier 3`	Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.
Step 5	**dampening** [*half-life-period reuse-threshold suppress-threshold max-suppress-time*] **Example:** `Device(config-bfd)# dampening 2 1000 3000 8`	Configures a device to dampen a flapping session.
Step 6	**end** **Example:** `Device(config-bfd)# end`	Exits BFD configuration mode and returns to privileged EXEC mode.
Step 7	**show bfd neighbors details** **Example:** `Device# show bfd neighbors details`	(Optional) Displays the listing of existing BFD adjacencies and the dampening information about the BFD sessions if BFD dampening is enabled for the session.
Step 8	**show bfd neighbors dampening** **Example:** `Device# show bfd neighbors dampening`	(Optional) Displays the dampening information about the BFD sessions configured with BFD dampening.
Step 9	**show bfd neighbors dampened** **Example:** `Device# show bfd neighbors dampened`	(Optional) Displays the dampening information about the BFD sessions that are currently dampened.

Configuration Examples for BFD Dampening

Example: Configuring BFD Dampening

The following example shows how to configure BFD dampening.

```
bfd-template multi-hop doctemplate
 interval min-tx 120 min-rx 100 multiplier 3
 dampening 2 1000 3000 8
```

Additional References for BFD Dampening

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
BFD commands	Cisco IOS IP Routing: Protocol-Independent Command Reference
Bidirectional Forwarding Detection	*IP Routing BFD Configuration Guide*

Technical Assistance

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

Feature Information for BFD Dampening

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

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

Table 10: Feature Information for BFD Dampening

Feature Name	Releases	Feature Information
BFD Dampening	Cisco IOS XE Release 3.8S	The BFD Dampening feature introduces a configurable exponential delay mechanism to suppress the excessive effect of remote node reachability events flapping with BFD. This feature also allows the network operator to automatically dampen a given BFD session to prevent excessive notification to the BFD clients, thus preventing unnecessary instability in the network. The following commands were introduced or modified: **dampening (bfd)** and **show bfd neighbors**.