Bidirectional Forwarding Detection

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.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Bidirectional Forwarding Detection" section on page 111.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Bidirectional Forwarding Detection

- Cisco Express Forwarding (CEF) and IP routing must be enabled on all participating routers.
- You must enable Cisco Parallel eXpress Forwarding (PXF) on the Cisco 10720 Internet router in order for BFD to operate properly. PXF is enabled by default and is generally not turned off.
- 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 on page 2 for more information on BFD routing protocol support in Cisco IOS software.

Restrictions for Bidirectional Forwarding Detection

- For the current Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE, 12.0(31)S, 12.4(4)T, 12.0(32)S, , 12.2(33)SRA, and 12.2(33)SRB, only asynchronous mode is supported. In asynchronous mode, either BFD peer can initiate a BFD session.
- For the current Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE, 12.0(31)S, 12.4(4)T, 12.0(32)S, 12.2(33)SRA, and 12.2(33)SRB, BFD is supported only for IPv4 networks.
- For Cisco IOS Release 12.2(33)SRB, the Cisco implementation of BFD supports only the following routing protocols: BGP, EIGRP, IS-IS, and OSPF.
- For Cisco IOS Release 12.2(33)SRA, the Cisco implementation of BFD supports only the following routing protocols: BGP, IS-IS, and OSPF.
- For Cisco IOS Release 12.4(4)T, the Cisco implementation of BFD supports only the following routing protocols: Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF).
- For Cisco IOS Release 12.4(11)T, the Cisco implementation of BFD introduced support for the Hot Standby Router Protocol (HSRP). BFD support is not available for all platforms and interfaces. In Cisco IOS Release 12.4(11)T, this feature was introduced on Cisco 7200 series, Cisco 7600 series, and Cisco 12000 series routers.
- For Cisco IOS Releases 12.0(31)S and 12.0(32)S, the Cisco implementation of BFD supports only the following routing protocols: BGP, IS-IS, and OSPF.
- For Cisco IOS Release 12.2(18)SXE, the Cisco implementation of BFD supports only the following routing protocols: EIGRP, IS-IS, and OSPF.
- BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away. Multihop configurations are not supported.
- 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.
- On the Cisco 10720 Internet router, BFD is supported only on Fast Ethernet, Gigabit Ethernet, and RPR-IEEE interfaces. BFD is not supported on Spatial Reuse Protocol (SRP) and Packet-over-SONET (POS) interfaces.

- When you configure the BFD session parameters on a Cisco 10720 interface using the **bfd** command (in interface configuration mode), the minimum configurable time period supported for the *milliseconds* argument in both the **interval** *milliseconds* and **min_rx** *milliseconds* parameters is 50 milliseconds.
- A maximum of 100 BFD sessions are supported on the Cisco 10720 Internet router. When BFD tries to set up a connection between routing protocols and establish a 101th session between a Cisco 10720 Internet router and adjacent routers, the following error message is displayed:

```
00:01:24: %OSPF-5-ADJCHG: Process 100, Nbr 10.0.0.0 on RPR-IEEE1/1 from LOADING to
FULL, Loading Done
00:01:24: %BFD-5-SESSIONLIMIT: Attempt to exceed session limit of 100 neighbors.
```

- The Cisco 10720 Internet router does not support the following BFD features:
  - Demand mode
  - Echo packets
  - BFD over IP Version 6
- On the Cisco 12000 series router, asymmetrical routing between peer devices may cause a BFD control packet to be received on a line card other than the line card that initiated the session. In this special case, the BFD session between the routing peers will not be established.
- A maximum 100 sessions per line card are supported for the distributed Cisco 12000 series Internet router. The minimum hello interval is 50 ms with up to three Max retries for a BFD control packet to be received from a remote system before a session with a neighbor is declared down.

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

Information About Bidirectional Forwarding Detection

Before you configure BFD, you should become familiar with the information in the following sections:

- BFD Operation, page 3
- Benefits of Using BFD for Failure Detection, page 6

BFD Operation

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Cisco supports the BFD asynchronous mode, which depends on the sending of BFD control packets between two systems to activate and maintain BFD neighbor sessions between routers. Therefore, in order for a BFD session to be created, you must configure BFD on both systems (or BFD peers). Once BFD has been enabled on the interfaces and at the router level for the appropriate routing protocols, a BFD session is created, BFD timers are negotiated, and the BFD peers will begin to send BFD control packets to each other at the negotiated interval.

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

Figure 1 Establishing a BFD Neighbor Relationship

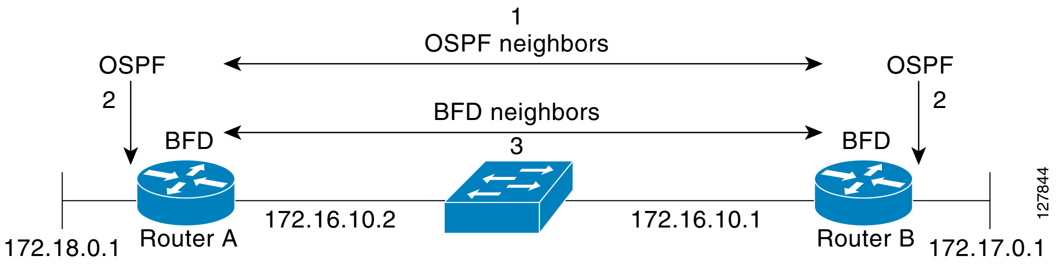
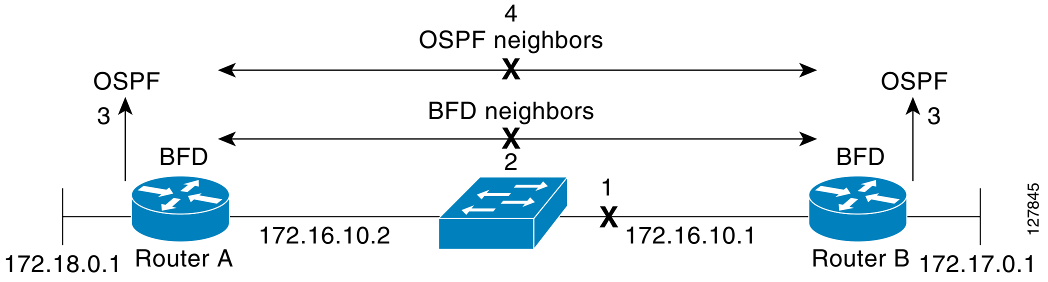


Figure 2 shows what happens when a failure occurs in the network (1). The BFD neighbor session with the OSPF neighbor router is torn down (2). BFD notifies the local OSPF process that the BFD neighbor is no longer reachable (3). The local OSPF process tears down the OSPF neighbor relationship (4). If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

Figure 2 Tearing Down an OSPF Neighbor Relationship



BFD Detection of Failures

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

- BFD is a forwarding path failure detection protocol. BFD detects a failure, but the routing protocol must take action to bypass a failed peer.
- Typically, BFD can be used at any protocol layer. However, the Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE, 12.0(31)S, and 12.4(4)T supports only Layer 3 clients, in particular, the BGP, EIGRP, IS-IS, and OSPF routing protocols.
- Cisco devices will use one BFD session for multiple client protocols in the Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE, 12.0(31)S, and 12.4(4)T. For example, if a network is running OSPF and EIGRP across the same link to the same peer, only one BFD session will be established, and BFD will share session information with both routing protocols.

BFD Version Interoperability

Cisco IOS Release 12.4(9)T supports BFD Version 1 as well as BFD Version 0. All BFD sessions come up as Version 1 by default and will be interoperable with Version 0. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, of one BFD neighbor is running BFD Version 0 and the other BFD neighbor is running Version 1, the session will run BFD Version 0. The output from the **show bfd neighbors** [**details**] command will verify which BFD version a BFD neighbor is running.

See the "Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default: Example" section on page 29 for an example of BFD version detection.

BFD Support on Cisco 12000 Routers

The Cisco 12000 series routers support distributed BFD to take advantage of its distributed Route Processor (RP) and line card (LC) architecture. The BFD tasks will be divided and assigned to the BFD process on RP and LC as described in the following sections:

- BFD Process on the RP
- BFD Process on the LC

BFD Process on the RP

Client Interaction

The BFD process on the RP will handle the interaction with clients, which create and delete BFD sessions.

Session Management for BFD Process on the RP

The BFD RP process will primarily own all BFD sessions on the router. It will pass the session creation and deletion requests to the BFD processes on all LCs. BFD LC sessions will have no knowledge of sessions being added or deleted by the clients. Only the BFD RP process will send session addition and deletion commands to the BFD LC process.

Session Database Management

The BFD RP process will maintain a database of all the BFD sessions on the router. This database will contain only the minimum required information.

Process EXEC Commands

The BFD RP process services the BFD **show** commands.

BFD Process on the LC

Session Management for BFD Process on the LC

The BFD LC process manages sessions, adds and deletes commands from the BFD RP process, and creates and deletes new sessions based on the commands. In the event of transmit failure, receive failure, or session down detection, the LC BFD instance will immediately notify the BFD RP process. It will also update transmit and receive counters. The BFD session is maintained completely on the LC. BFD control packets are received and processed, as well as sent, from the LC itself.

Database Management

The BFD LC process maintains a database of all the BFD sessions hosted on the LC.

Receive and Transmit

The BFD LC process is responsible for transmitting and receiving BFD packets for the sessions on the LC.

Benefits of Using BFD for Failure Detection

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

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

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

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

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

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

How to Configure Bidirectional Forwarding Detection

You start a BFD process by configuring BFD on the interface. When the BFD process is started, no entries are created in the adjacency database, in other words, no BFD control packets are sent or received. BFD echo mode, which is supported in BFD Version 1 for Cisco IOS 12.4(9)T, is enabled by default. BFD echo packets are sent and received in addition to BFD control packets. The adjacency creation takes places once you have configured BFD support for the applicable routing protocols. This section contains the following procedures:

- Configuring BFD Session Parameters on the Interface, page 7 (required)
- Configuring BFD Support for Routing Protocols, page 7 (required)
- Configuring BFD Echo Mode, page 22 (optional)
- Monitoring and Troubleshooting BFD, page 25 (optional)

Configuring BFD Session Parameters on the Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

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	**`bfd interval`** *`milliseconds`* **`min_rx`** *`milliseconds`* **`multiplier`** *`interval-multiplier`*
	Example:
	`Router(config-if)# bfd interval 50 min_rx 50 multiplier 5`
		Enables BFD on the interface.

Step 5	**`end`**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode.

Configuring BFD Support for Routing Protocols

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

For Cisco IOS Release 12.2(18)SXE, you must configure BFD support for one or more of the following routing protocols: EIGRP, IS-IS, and OSPF.

For Cisco IOS Releases 12.2(33)SRA, you must configure BFD support for one or more of the following routing protocols: EIGRP, IS-IS, and OSPF.

For Cisco IOS Releases 12.2(33)SRB, you must configure BFD support for one or more of the following routing protocols: BGP, EIGRP, IS-IS, and OSPF.

For Cisco IOS Releases 12.0(31)S and 12.4(4)T, you must configure BFD support for one or more of the following routing protocols: BGP, IS-IS, and OSPF.

For Cisco IOS Release 12.0(32)S, for the Cisco 10720 platform, you must configure BFD for one or more of the following routing protocols: BGP, IS-IS, and OSPF.

For Cisco IOS Release 12.4(11)T, BFD support for HSRP was introduced.

This section describes the following procedures:

- Configuring BFD Support for BGP, page 8 (optional)
- Configuring BFD Support for EIGRP, page 10 (optional)
- Configuring BFD Support for IS-IS, page 12 (optional)
- Configuring BFD Support for OSPF, page 16 (optional)
- Configuring BFD Support for HSRP, page 20 (optional)

Configuring BFD Support for BGP

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

Prerequisites

BGP must be running on all participating 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 on page 7 for more information.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`router bgp`** *`as-tag`*
	Example:
	`Router(config)# router bgp tag1`
		Specifies a BGP process and enters router configuration mode.

Step 4	**`neighbor`** *`ip-address`* **`fall-over bfd`**
	Example:
	`Router(config-router)# neighbor 172.16.10.2 fall-over bfd`
		Enables BFD support for fallover.

Step 5	**`end`**
	Example:
	`Router(config-router)# end`
		Returns the router to privileged EXEC mode.

Step 6	**`show bfd neighbors`** `[`**`details`**`]`
	Example:
	`Router# show bfd neighbors detail`
		Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered.
		Note In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details** command when it is entered on a line card.

Step 7	**`show ip bgp neighbor`**
	Example:
	`Router# show ip bgp neighbor`
		Displays information about BGP and TCP connections to neighbors.

What to Do Next

See the "Monitoring and Troubleshooting BFD" section on page 25 for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections:

- Configuring BFD Support for EIGRP, page 10
- Configuring BFD Support for IS-IS, page 12

- Configuring BFD Support for OSPF, page 16
- Configuring BFD Support for HSRP, page 20

Configuring BFD Support for EIGRP

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

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

Prerequisites

EIGRP must be running on all participating 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 on page 7 for more information.

Restrictions

BFD for EIGRP is not supported on the Cisco 12000 series routers for Cisco IOS Releases 12.0(31)S, 12.0(32)S, 12.4(4)T, and 12.2(33)SRA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **log-adjacency-changes** [**detail**]
5. **bfd all-interfaces**
   or
   bfd interface *type number*
6. **end**
7. **show bfd neighbors** [**details**]
8. **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	**`log-adjacency-changes`** [**`detail`**] **Example:** `Router(config-router)# log-adjacency-changes`	Configures the router to send a system logging (syslog) message when an EIGRP neighbor goes up or down. • Entering the **log-adjacency-changes** command allows you to see the "BFD node down" syslog message whenever a neighbor is down due to receiving a BFD failure detection notification.

Step 5	**`bfd all-interfaces`**
	or
	`bfd interface` *`type number`*
	Example:
	`Router(config-router)# bfd all-interfaces`
	or
	Example:
	`Router(config-router)# bfd interface FastEthernet 6/0`
		Enables BFD globally on all interfaces associated with the EIGRP routing process.
		or
		Enables BFD on a per-interface basis for one or more interfaces associated with the EIGRP routing process.

Step 6	`end`
	Example:
	`Router(config-router) end`
		Returns the router to privileged EXEC mode.

	Command or Action	Purpose
Step 7	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** In order to see the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details** command when it is entered on a line card.
Step 8	**show ip eigrp interfaces** [*type number*] [*as-number*] [**detail**] **Example:** `Router# show ip eigrp interfaces detail`	Displays the interfaces for which BFD support for EIGRP has been enabled.

What to Do Next

See the "Monitoring and Troubleshooting BFD" section on page 25 for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections:

- Configuring BFD Support for BGP, page 8
- Configuring BFD Support for IS-IS, page 12
- Configuring BFD Support for OSPF, page 16
- Configuring BFD Support for HSRP, page 20

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 for which IS-IS is 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:

- Configuring BFD Support for IS-IS for All Interfaces, page 13
- Configuring BFD Support for IS-IS for One or More Interfaces, page 14

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 on page 7 for more information.

Configuring BFD Support for IS-IS for All Interfaces

To configure BFD on all IS-IS interfaces, 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. **isis bfd** [**disable**]
8. **end**
9. **show bfd neighbors** [**details**]
10. **show clns interface**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`router isis` *area-tag* **Example:** `Router(config)# router isis tag1`	Specifies an IS-IS process and enters router configuration mode.

Step 4	`bfd all-interfaces`
	Example:
	`Router(config-router)# bfd all-interfaces`
		Enables BFD globally on all interfaces associated with the IS-IS routing process.

Step 5	`exit`
	Example:
	`Router(config-router)# exit`
		(Optional) Returns the router to global configuration mode. Enter this command only if you want to follow Step 6 and Step 7 to disable BFD for one or more interfaces.

	Command or Action	Purpose
Step 6	**interface** *type number* Example: `Router(config)# interface fastethernet 6/0`	(Optional) Enters interface configuration mode.
Step 7	**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 8	**end**
	Example:
	`Router(config-if)# end`
		Returns the router to privileged EXEC mode.

Step 9	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	Displays information that can be used to verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details** command when it is entered on a line card.
Step 10	**show clns interface** **Example:** `Router# show clns interface`	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 on page 25 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 on page 14.

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isis bfd** [**disable**]
5. **end**

6. **show bfd neighbors** [**details**]
7. **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	**`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 5	**`end`**
	Example:
	`Router(config-if)# end`
		Returns the router to privileged EXEC mode.

Step 6	**`show bfd neighbors`** `[`**`details`**`]`
	Example:
	`Router# show bfd neighbors details`
		Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.
		Note In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details** command when it is entered on a line card.

Step 7	**`show clns interface`**
	Example:
	`Router# show clns interface`
		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 on page 25 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 BGP, page 8
- Configuring BFD Support for EIGRP, page 10
- Configuring BFD Support for OSPF, page 16
- Configuring BFD Support for HSRP, page 20

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, page 16 (optional)
- Configuring BFD Support for OSPF for One or More Interfaces, page 18 (optional)

Configuring BFD Support for OSPF for All Interfaces

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

If you do not want to configure BFD on all OSPF interfaces and would rather configure BFD support specifically for one or more interfaces, see the "Configuring BFD Support for OSPF for One or More Interfaces" section on page 18.

Prerequisites

OSPF must be running on all participating routers.

The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured. See the "Configuring BFD Session Parameters on the Interface" section on page 7 for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **bfd all-interfaces**

5. **exit**
6. **interface** *name 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:
	`Router(config)# router ospf 4`
		Specifies an OSPF process and enters router configuration mode.

Step 4	**`bfd all-interfaces`**
	Example:
	`Router(config-router)# bfd all-interfaces`
		Enables BFD globally on all interfaces associated with the OSPF routing process.

Step 5	**`exit`**
	Example:
	`Router(config-router)# exit`
		(Optional) Returns 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`
		Returns the router to privileged EXEC mode.

	Command or Action	Purpose

Step 9	`show bfd neighbors [details]`
	Example:
	`Router# show bfd neighbors detail`
		Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.
		Note In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details** command when it is entered on a line card.

Step 10	`show ip ospf`
	Example:
	`Router# show ip ospf`
		Displays information that can help verify if BFD for OSPF has been enabled.

What to Do Next

See the "Monitoring and Troubleshooting BFD" section on page 25 for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections:

- Configuring BFD Support for BGP, page 8
- Configuring BFD Support for EIGRP, page 10
- Configuring BFD Support for IS-IS, page 12
- Configuring BFD Support for HSRP, page 20

Configuring BFD Support for OSPF for One or More Interfaces

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

Prerequisites

OSPF must be running on all participating routers.

The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured. See the "Configuring BFD Session Parameters on the Interface" section on page 7 for more information.

SUMMARY STEPS

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

DETAILED STEPS

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

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Returns the router to privileged EXEC mode.

Step 6	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details** command when it is entered on a line card.
Step 7	**show ip ospf** **Example:** `Router# show ip ospf`	Displays information that can help verify if BFD support for OSPF has been enabled.

What to Do Next

See the "Monitoring and Troubleshooting BFD" section on page 25 for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections:

- Configuring BFD Support for BGP, page 8
- Configuring BFD Support for EIGRP, page 10
- Configuring BFD Support for IS-IS, page 12
- Configuring BFD Support for HSRP, page 20

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.

Prerequisites

- HSRP must be running on all participating routers.
- Cisco Express Forwarding (CEF) 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 CEF or distributed CEF.
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.
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.

	Command or Action	Purpose
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 on page 25 for more information on monitoring and troubleshooting BFD. If you want to configure BFD support for another routing protocol, see the following sections:

- Configuring BFD Support for BGP, page 8
- Configuring BFD Support for EIGRP, page 10
- Configuring BFD Support for IS-IS, page 12
- Configuring BFD Support for OSPF, page 16

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. Before you configure echo mode you should be familiar with the following concepts:

- BFD Echo Mode, page 22
- Prerequisites, page 23
- Restrictions, page 23

BFD Echo Mode

Benefits of Running BFD Echo Mode

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

Echo Mode Without Asymmetry

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

Prerequisites

BFD must be running on all participating routers.

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

The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured. See the "Configuring BFD Session Parameters on the Interface" section on page 7 for more information.

Restrictions

BFD echo mode which is supported in BFD Version 1, is available only in Cisco IOS Releases 12.4(9)T and 12.2(33)SRA.

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

- Configuring the BFD Slow Timer, page 23
- Disabling BFD Echo Mode Without Asymmetry, page 24

Configuring the BFD Slow Timer

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**bfd slow-timer** *milliseconds* **Example:** `Router(config)# bfd slow-timer 12000`	Configures the BFD slow timer.

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits interface configuration 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. [**no**] **bfd echo**
4. **bfd echo**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **bfd echo** **Example:** `Router(config)# no bfd echo`	Disables BFD echo mode.

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode.

Monitoring and Troubleshooting BFD

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

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

This section contains information for monitoring and troubleshooting BFD for the following Cisco platforms:

- Monitoring and Troubleshooting BFD for Cisco 7600 Series Routers, page 25
- Monitoring and Troubleshooting BFD for Cisco 12000 Series Routers, page 26
- Monitoring and Troubleshooting BFD for Cisco 10720 Internet Routers, page 28

Monitoring and Troubleshooting BFD for Cisco 7600 Series Routers

To monitor or troubleshoot BFD on Cisco 7600 series routers, perform one or more of the steps in this section.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`show bfd neighbors`** `[`**`details`**`]`
	Example:
	`Router# show bfd neighbors details`
		Displays the BFD adjacency database.
		- The **details** keyword shows all BFD protocol parameters and timers per neighbor.
		Note In order to see the full output of the **show bfd neighbors details** command on a a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details** command when it is entered on a line card.

Step 3	**`debug bfd`** `[`**`packet`** `|` **`event`**`]`
	Example:
	`Router# debug bfd packet`
		Displays debugging information about BFD packets.

Monitoring and Troubleshooting BFD for Cisco 12000 Series Routers

To monitor or troubleshoot BFD on Cisco 12000 series routers, perform one or more of the steps in this section.

SUMMARY STEPS

1. **enable**
2. **attach** *slot-number*
3. **show bfd neighbors** [**details**]
4. **show monitor event-trace bfd** [**all**]
5. **debug bfd event**
6. **debug bfd packet**
7. **debug bfd ipc-error**
8. **debug bfd ipc-event**
9. **debug bfd oir-error**
10. **debug bfd oir-event**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**attach** *slot-number* **Example:** `Router# attach 6`	Connects you to a specific line card for the purpose of executing monitoring and maintenance commands on the specified line card. Slot numbers range from 0 to 11 for the Cisco 12012 and from 0 to 7 for the Cisco 12008. • If the slot number is omitted, you are prompted for the slot number. **Note** In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card.
Step 3	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	Displays the BFD adjacency database. • The **details** keyword shows all BFD protocol parameters and timers per neighbor. **Note** The registered protocols are not shown in the output of the **show bfd neighbors details** when it is entered on a line card.
Step 4	**show monitor event-trace bfd** [**all**] **Example:** `Router# show monitor event-trace bfd all`	Displays logged messages for important events in "recent past" on BFD activities that occur on the line cards. This is a rolling buffer based log, so "distant past" events would be lost. Depending on traffic and frequency of events, these events could be seen over a variable time window.

Step 5	`debug bfd event`
	Example:
	`Router# debug bfd event`
		Displays debugging information about BFD state transitions.

Step 6	`debug bfd packet`
	Example:
	`Router# debug bfd packet`
		Displays debugging information about BFD control packets.

Step 7	`debug bfd ipc-error`
	Example:
	`Router# debug bfd ipc-error`
		Displays debugging information with IPC errors on the RP and LC.

Step 8	`debug bfd ipc-event`
	Example:
	`Router# debug bfd ipc-event`
		Displays debugging information with IPC events on the RP and LC.

	Command or Action	Purpose

Step 9	**`debug bfd oir-error`**
	Example:
	`Router# debug bfd oir-error`
		Displays debugging information with OIR errors on the RP and LC.

Step 10	**`debug bfd oir-event`**
	Example:
	`Router# debug bfd oir-event`
		Displays debugging information with OIR events on the RP and LC.

Monitoring and Troubleshooting BFD for Cisco 10720 Internet Routers

To monitor or troubleshoot BFD on Cisco 10720 Internet routers, perform one or more of the steps in this section.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**`show bfd neighbors`** [**`details`**] **Example:** `Router# show bfd neighbors details`	(Optional) Displays the BFD adjacency database. • The **details** keyword will show all BFD protocol parameters and timers per neighbor. **Note** The registered protocols are not shown in the output of the **show bfd neighbors details** when it is entered on a line card.

Step 3	**`debug bfd event`**
	Example:
	`Router# debug bfd event`
		Displays debugging information about BFD state transitions.

Step 4	**`debug bfd packet`**
	Example:
	`Router# debug bfd packet`
		Displays debugging information about BFD control packets.

Configuration Examples for Bidirectional Forwarding Detection

This section provides the following configuration examples:

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

12.4(9)T Example

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

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

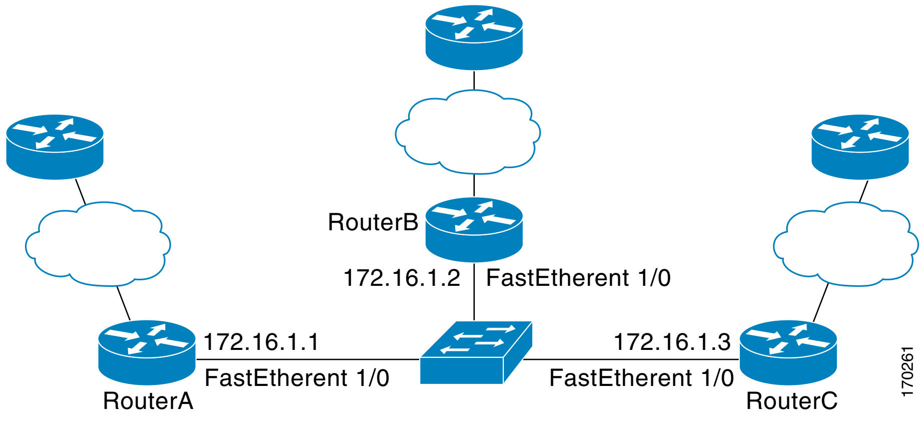


Figure 3 shows a large EIGRP network with several routers, three of which are BFD neighbors that are running EIGRP as their routing protocol.

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

Configuration for RouterA

```
interface FastEthernet0/0
 no shutdown
 ip address 10.4.9.14 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 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 171.16.1.129 255.255.255.255 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 FastEthernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 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 171.16.1.129 255.255.255.255 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 FastEthernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.1.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 no shutdown
 duplex auto
 speed auto

!
router eigrp 11
 network 172.16.0.0
 bfd all-interfaces
 auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 171.16.1.129 255.255.255.255 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

```
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   Fa0/1
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(1364284)
Rx Count: 1351813, Rx Interval (ms) min/max/avg: 28/64/49 last: 4 ms ago
Tx Count: 1364289, Tx Interval (ms) min/max/avg: 40/68/49 last: 32 ms ago
Registered protocols: EIGRP
Uptime: 18:42:45
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 3          - Your Discr.: 5
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.1    172.16.1.2     6/1    Up        0    (3 )   Up        Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(317)
Rx Count: 305, Rx Interval (ms) min/max/avg: 1/1016/887 last: 448 ms ago
Tx Count: 319, Tx Interval (ms) min/max/avg: 1/1008/880 last: 532 ms ago
Registered protocols: EIGRP
Uptime: 00:04:30
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 1          - Your Discr.: 6
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

The output from the **show bfd neighbors details** command on 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.

Router B

```
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        Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.3     3/6    1(RH)     118  (3 )   Up        Fa0/1
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(5735)
Rx Count: 5731, Rx Interval (ms) min/max/avg: 32/72/49 last: 32 ms ago
Tx Count: 5740, Tx Interval (ms) min/max/avg: 40/64/50 last: 44 ms ago
Registered protocols: EIGRP
Uptime: 00:04:45
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 3
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0
```

Figure 4 Fast Ethernet interface 0/1 Failure

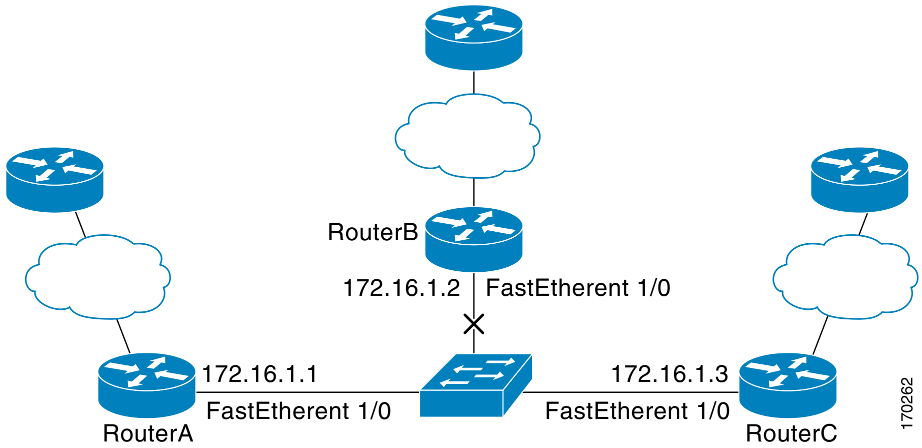


Figure 4 shows a that Fast Ethernet interface 0/1 on RouterB has failed. Without this neighbor, there is no way to reach the network beyond RouterB.

When Fast Ethernet interface 0/1 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 0/1 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        Fa0/1
```

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        Fa0/1
```

Configuring BFD in an OSPF Network: Example

12.0(31)S

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 FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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 FastEthernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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:

Note Router B is a Cisco 12000 series router. The **show bfd neighbors details** command must be run on the line cards. The **show bfd neighbors details** command will not display the registered protocols when it is entered on a line card.

```
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!

LC-Slot6> 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 fastethernet 0/1

show ip ospf interface fastethernet 0/1
FastEthernet0/1 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 fastethernet 6/1

FastEthernet6/1 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)
```

Configuring BFD in a BGP Network: Example

12.0(31)S

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 FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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 FastEthernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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:

Note Router B is a Cisco 12000 series router. The **show bfd neighbors details** command must be run on the line cards. The **show bfd neighbors details** command will not display the registered protocols when it is entered on a line card.

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!

LC-Slot6> 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
.
.
.
```

Configuring BFD in an IS-IS Network: Example

12.0(31)S

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 FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
ip router isis
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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 FastEthernet 6/0
```

```
 ip address 172.16.10.2 255.255.255.0
ip router isis
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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:

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   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:

Note Router B is a Cisco 12000 series router. The **show bfd neighbors details** command must be run on the line cards. The **show bfd neighbors details** command will not display the registered protocols when it is entered on a line card.

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!

LC-Slot6> 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
```

Configuring BFD in an HSRP Network: Example

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 FastEthernet2/0
 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 FastEthernet2/0
 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 FastEthernet2/0
  10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !

RouterB# show standby neighbors

HSRP neighbors on FastEthernet2/0
  10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled !
```

Additional References

The following sections provide references related to the BFD feature.

Related Documents

Related Topic	**Document Title**
Configuring and monitoring BGP	"BGP" module of the *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4
Configuring and monitoring EIGRP	"EIGRP" module of the *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4
Configuring and monitoring IS-IS	"Configuring Integrated IS-IS" module of the *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4
Configuring and monitoring OSPF	"OSPF" module of the *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4
Configuring and monitoring HSRP	"Configuring HSRP" module of the *Cisco IOS IP Application Services Configuration Guide*, Release 12.4T

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

New Commands in Cisco IOS Release 12.2(18)SXE

- bfd
- bfd all-interfaces
- bfd interface
- debug bfd
- ip ospf bfd
- isis bfd
- show bfd neighbors

Modified Commands in Cisco IOS Release 12.2(18)SXE

- show clns interface
- show ip eigrp interfaces
- show ip ospf
- show monitor event-trace

New Commands in Cisco IOS Release 12.0(31)S

- bfd
- bfd all-interfaces
- bfd interface
- debug bfd
- ip ospf bfd
- isis bfd
- show bfd neighbors

Modified Commands in Cisco IOS Release 12.0(31)S

- show monitor event-trace
- show ip bgp neighbors
- show ip ospf
- show monitor event-trace

New Commands in Cisco IOS Release 12.4(4)T

- bfd
- bfd all-interfaces
- bfd interface
- debug bfd
- ip ospf bfd
- isis bfd
- show bfd neighbors

Modified Commands in Cisco IOS Release 12.4(4)T

- **show clns interface**
- **show ip bgp neighbors**
- **show ip ospf**
- **show monitor event-trace**

New Commands in Cisco IOS Release 12.0(32)S

- None

Modified Commands in Cisco IOS Release 12.0(32)S

- None

New Commands in Cisco IOS Release 12.2(33)SRA

- None

Modified Commands in Cisco IOS Release 12.2(33)SRA

- None

Modified Commands in Cisco IOS Release 12.2(33)SRB

- None

New Commands in Cisco IOS Release 12.4(9)T

- **bfd echo**
- **bfd slow-timer**

Modified Commands in Cisco IOS Release 12.4(9)T

- **show bfd neighbors**

New Commands in Cisco IOS Release 12.4(11)T

- **show standby neighbors**
- **standby bfd**
- **standby bfd all-interfaces**

Modified Commands in Cisco IOS Release 12.4(11)T

- **show standby**

bfd

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Syntax Description

interval *milliseconds*	Specifies the rate at which BFD control packets will be sent to BFD peers. The configurable time period for the *milliseconds* argument is from 50 to 999 milliseconds (ms).
min_rx *milliseconds*	Specifies the rate at which BFD control packets will be expected to be received from BFD peers. The configurable time period for the *milliseconds* argument is from 1 to 999 milliseconds (ms).
multiplier *multiplier-value*	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The configurable value range for the *multiplier-value* argument is from 3 to 50.

Command Default

No baseline BFD session parameters are set.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows the BFD session parameters set for FastEthernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# bfd interval 50 min_rx 2 multiplier 3
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.
clear bfd	Clears BFD session parameters.
ip ospf bfd	Enables BFD on a specific interface configured for OSPF.

bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration mode. To disable BFD for all interfaces, use the **no** form of this command.

bfd all-interfaces

no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on the interfaces participating in the routing process.

Command Modes

Router configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There are two methods to configure routing protocols to use BFD for failure detection. To enable BFD for all neighbors of a routing protocol, enter the **bfd all-interfaces** command in router configuration mode. If you do not want to enable BFD on all interfaces, enter the **bfd interface** command in router configuration mode.

Examples

The following example shows BFD enabled for all Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

The following example shows BFD enabled for all Intermediate System-to-Intermediate System (IS-IS) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router isis tag1
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

The following example shows BFD enabled for all Open Shortest Path First (OSPF) neighbors:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
bfd interface	Enables BFD on a per-interface basis for a BFD peer.

bfd echo

To enable Bidirectional Forwarding Detection (BFD) echo mode, use the **bfd echo** command in interface configuration mode. To disable BFD echo mode, use the **no** form of this command.

bfd echo

no bfd echo

Syntax Description

This command has no arguments or keywords.

Command Default

BFD echo mode is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Echo mode is enabled by default. Entering the **no bfd echo** command without any keywords turns off the sending of echo packets and signifies that the router is unwilling to forward echo packets received from BFD neighbor routers.

When echo mode is enabled, the desired minimum echo transmit interval and required minimum transmit interval values are taken from the **bfd interval** *milliseconds* **min_rx** *milliseconds* parameters, respectively.

Note If the **no ip route-cache same-interface** command is configured, the **bfd echo accept** command will not be accepted.

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

Echo Mode Without Asymmetry

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

Examples

The following example configures echo mode between BFD neighbors.

```
Router> enable
Router# configure terminal
Router(config)# interface Ethernet 0/1
Router(config-if)# bfd echo
```

The following output from the **show bfd neighbors details** command shows that the BFD session neighbor is up and using BFD echo mode. The relevant command output is shown in bold in the output.

```
Router# 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       Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on the interface.
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
ip route-cache	Controls the use of switching methods for forwarding IP packets.

bfd interface

To enable Bidirectional Forwarding Detection (BFD) on a per-interface basis for a BFD peer, use the **bfd interface** command in router configuration mode. To disable BFD on a per-interface basis, use the **no** form of this command.

bfd interface *type number*

no bfd interface *type number*

Syntax Description

type	Interface type for the interface to be enabled for BFD.
number	Interface number for the interface to be enabled for BFD.

Command Default

BFD is not enabled on the interface.

Command Modes

Router configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There are two methods to configure routing protocols to use BFD for failure detection. To enable BFD for all neighbors of a routing protocol, enter the **bfd all-interfaces** command in router configuration mode. If you do not want to enable BFD on all interfaces, enter the **bfd interface** command in router configuration mode.

Examples

The following example shows BFD enabled for the Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor Fast Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 123
Router(config-router)# bfd interface fastethernet 3/0
Router(config-if)# end
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.

bfd slow-timer

To configure the Bidirectional Forwarding Detection (BFD) slow timer value, use the **bfd slow-timer** command in global configuration mode. This command does not have a **no** form.

bfd slow-timer [*milliseconds*]

Syntax Description

milliseconds	(Optional) BFD slow timer value, in milliseconds. Range is from 1000 30000. If unspecified, the default is 1000.

Command Default

The BFD slow timer value is 1000 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

In the following example, the BFD slow timer value is configured to 14,000 milliseconds.

```
Router(config)# bfd slow-timer 14000
```

The following output from the **show bfd neighbors details** command shows that the BFD slow timer value of 14,000 milliseconds has been implemented. The values for the MinTxInt and MinRxInt will correspond to the configured value for the BFD slow timer. The relevant command output is shown in bold.

```
Router# show bfd neighbors details

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.10.1   172.16.10.2   1/1    Up      0    (3 )      Up        Et2/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 14000, MinRxInt: 14000, Multiplier: 3
Received MinRxInt: 10000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(418)
Rx Count: 422, Rx Interval (ms) min/max/avg: 1/1480/1087 last: 112 ms ago
Tx Count: 420, Tx Interval (ms) min/max/avg: 1/2088/1090 last: 872 ms ago
Registered protocols: OSPF
Uptime: 00:07:37
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 1          - Your Discr.: 1
             Min tx interval: 14000 - Min rx interval: 14000
             Min Echo interval: 4000
```

Related Commands

Command	Description
bfd echo	Reenables echo mode if the **no bfd echo** command had been entered.

debug bfd

To display debugging messages about Bidirectional Forwarding Detection (BFD), use the **debug bfd** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

Cisco IOS Release 12.2(18)SXE, 12.4(4)T, and 12.2(33)SRA

debug bfd {**event** | **packet** [*ip-address*]}

no debug bfd {**event** | **packet** [*ip-address*]}

Cisco IOS Release 12.0(31)S

debug bfd {**event** | **packet** [*ip-address*] | **ipc-erro**r | **ipc-event** | **oir-error** | **oir-event**}

no debug bfd {**event** | **packet** [*ip-address*] | **ipc-erro**r | **ipc-event** | **oir-error** | **oir-event**}

Syntax Description

event	(Optional) Displays debugging information about BFD state transitions.
packet	(Optional) Displays debugging information about BFD control packets.
ip-address	(Optional) Displays debugging information about BFD only for the specified IP address.
ipc-error	(Optional) Displays debugging information with interprocess communication (IPC) errors on the Route Processor (RP) and line card (LC).
ipc-event	(Optional) Displays debugging information with IPC events on the RP and LC.
oir-error	(Optional) Displays debugging information with online insertion and removal (OIR) errors on the RP and LC.
oir-event	(Optional) Displays debugging information with OIR events on the RP and LC.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **debug bfd** command can be used to troubleshoot the BFD feature.

Note Because BFD is designed to send and receive packets at a very high rate, consider the potential effect on system resources before enabling this command, especially if there are a large number of BFD peers. The **debug bfd packet** command should be enabled only on a live network at the direction of Cisco Technical Assistance Center personnel.

Examples

The following example shows output from the **debug bfd packet** command. The IP address has been specified in order to limit the packet information to one interface:

```
Router# debug bfd packet 172.16.10.5

BFD packet debugging is on
*Jan 26 14:47:37.645: Tx*IP: dst 172.16.10.1, plen 24. BFD: diag 2, St/D/P/F (1/0/0/0),
mult 5, len 24, loc/rem discr 1 1, tx 1000000, rx 1000000 100000, timer 1000 ms, #103
*Jan 26 14:47:37.645: %OSPF-5-ADJCHG: Process 10, Nbr 172.16.10.12 on Ethernet1/4 from
FULL to DOWN, Neighbor Down: BFD node down
*Jan 26 14:47:50.685: %OSPF-5-ADJCHG: Process 10, Nbr 172.16.10.12 on Ethernet1/4 from
LOADING to FULL, Loading Done
*Jan 26 14:48:00.905: Rx  IP: src 172.16.10.1, plen 24. BFD: diag 0, St/D/P/F (1/0/0/0),
mult 4, len 24, loc/rem discr 2 1, tx 1000000, rx 1000000 100000, timer 4000 ms, #50
*Jan 26 14:48:00.905: Tx IP: dst 172.16.10.1, plen 24. BFD: diag 2, St/D/P/F (2/0/0/0),
mult 5, len 24, loc/rem discr 1 2, tx 1000000, rx 1000000 100000, timer 1000 ms, #131
*Jan 26 14:48:00.905: Rx  IP: src 172.16.10.1, plen 24. BFD: diag 0, St/D/P/F (3/0/0/0),
mult 4, len 24, loc/rem discr 2 1, tx 1000000, rx 1000000 100000, timer 4000 ms, #51
*Jan 26 14:48:00.905: Tx IP: dst 172.16.10.1, plen 24. BFD: diag 0, St/D/P/F (3/0/0/0),
mult 5, len 24, loc/rem discr 1 2, tx 1000000, rx 1000000 100000, timer 1000 ms, #132
```

The following example shows output from the **debug bfd event** command when an interface between two BFD neighbor routers fails and then comes back online:

```
Router# debug bfd event

22:53:48: BFD: bfd_neighbor - action:DESTROY, proc:1024, idb:FastEthernet0/1,
neighbor:172.16.10.2
22:53:48: BFD: bfd_neighbor - action:DESTROY, proc:512, idb:FastEthernet0/1,
neighbor:172.16.10.2
22:53:49: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event DETECT TIMER EXPIRED, state UP
-> FAILING
.
.
.
22:56:35: BFD: bfd_neighbor - action:CREATE, proc:1024, idb:FastEthernet0/1,
neighbor:172.16.10.2
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event RX IHY 0, state FAILING -> DOWN
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event RX IHY 0, state DOWN -> INIT
22:56:37: Session [172.16.10.1,172.16.10.2,Fa0/1,1], event RX IHY 1, state INIT -> UP
```

Table 1 describes the significant fields shown in the display.

Table 1 debug bfd event Field Descriptions

Field	Description
bfd_neighbor - action:DESTROY	The BFD neighbor will tear down the BFD session.
Session [172.16.10.1, 172.16.10.2, Fa0/1,1]	IP addresses of the BFD neighbors holding this session that is carried over FastEthernet interface 0/1.

Table 1 debug bfd event Field Descriptions (continued)

Field	Description
event DETECT TIMER EXPIRED	The BFD neighbor has not received BFD control packets within the negotiated interval and the detect timer has expired.
state UP -> FAILING	The BFD event state is changing from Up to Failing.
Session [172.16.10.1, 172.16.10.2, Fa0/1,1], event RX IHY 0	The BFD session between the neighbors indicated by the IP addresses that is carried over FastEthernet interface 0/1 is changing state from Failing to Down. The I Hear You (IHY) bit value is shown as 0 to indicate that the remote system is tearing down the BFD session.
event RX IHY 0, state DOWN -> INIT	The BFD session is still considered down, and the IHY bit value still is shown as 0, and the session state changes from DOWN to INIT to indicate that the BFD session is again initializing, as the interface comes back up.
event RX IHY 1, state INIT -> UP	The BFD session has been reestablished, and the IHY bit value changes to 1 to indicate that the session is live. The BFD session state changes from INIT to UP.

The following example shows output from the **debug bfd packet** command when an interface between two BFD neighbor routers fails and then comes back online. The diagnostic code changes from 0 (No Diagnostic) to 1 (Control Detection Time Expired) because no BFD control packets could be sent (and therefore detected by the BFD peer) after the interface fails. When the interface comes back online, the diagnostic code changes back to 0 to signify that BFD packets can be sent and received by the BFD peers.

```
Router# debug bfd packet

23:03:25: Rx  IP: src 172.16.10.2, plen 24. BFD: diag 0, H/D/P/F (0/0/0/0), mult 3, len
24, loc/rem discr 5 1, tx 1000000, rx 100007
23:03:25: Tx IP: dst 172.16.10.2, plen 24. BFD: diag 1, H/D/P/F (0/0/0/0), mult 5, len 24,
loc/rem discr 1 5, tx 1000000, rx 1000008
23:03:25: Tx IP: dst 172.16.10.2, plen 24. BFD: diag 1, H/D/P/F (1/0/0/0), mult 5, len 24,
loc/rem discr 1 5, tx 1000000, rx 1000009
```

Table 2 describes the significant fields shown in the display.

Table 2 debug bfd packet Field Descriptions

Field	Description
Rx IP: src 172.16.10.2	The router has received this BFD packet from the BFD router with source address 172.16.10.2.
plen 24	Length of the BFD control packet, in bytes.

Table 2 debug bfd packet Field Descriptions (continued)

Field	Description
diag 0	A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. State values are as follows: • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down
H/D/P/F (0/0/0/0)	H bit—Hear You bit. This bit is set to 0 if the transmitting system either is not receiving BFD packets from the remote system or is tearing down the BFD session. During normal operation the I Hear You bit is set to 1. D bit—Demand Mode bit. If the Demand Mode bit set, the transmitting system wants to operate in demand mode. BFS has two modes—asynchronous and demand. The Cisco implementation of BFD supports only asynchronous mode. P bit—Poll bit. If the Poll bit is set, the transmitting system is requesting verification of connectivity or of a parameter change. F bit—Final bit. If the Final bit is set, the transmitting system is responding to a received BFC control packet that had a Poll (P) bit set.
mult 3	Detect time multiplier. The negotiated transmit interval, multiplied by the detect time multiplier, determines the detection time for the transmitting system in BFD asynchronous mode. The detect time multiplier is similar to the hello multiplier in IS-IS, which is used to determine the holdtimer: (hellointerval) * (hellomultiplier) = holdtimer. If a hello packet is not received within the hold-timer interval, a failure has occurred. Similarly, 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.
len 24	The BFD packet length.

Table 2 debug bfd packet Field Descriptions (continued)

Field	Description
loc/rem discr 5 1	The values for My Discriminator (local) and Your Discriminator (remote) BFD neighbors. • My Discriminator—Unique, nonzero discriminator value generated by the transmitting system, used to demultiplex multiple BFD sessions between the same pair of systems. • Your Discriminator—The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator, or is zero if that value is unknown.
tx 1000000	Desired minimum transmit interval.
rx 100007	Required minimum receive interval.

ip ospf bfd

To enable Bidirectional Forwarding Detection (BFD) on a specific interface configured for Open Shortest Path First (OSPF), use the **ip ospf bfd** command in interface configuration mode. To disable BFD on the OSPF interface, use the **disable** keyword. To remove the **ospf bfd** command, use the **no** form of this command.

ip ospf bfd [**disable**]

no ip ospf bfd

Syntax Description

disable	(Optional) Disables BFD for OSPF on a specified interface.

Defaults

When the **disable** keyword is not used, the default behavior is to enable BFD support for OSPF on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Enter the **ip ospf bfd** command to configure an OSPF interface to use BFD for failure detection. If you have used the **bfd-all interfaces** command in router configuration mode to globally configure all OSPF interfaces for an OSPF process to use BFD, you can enter the **ip ospf bfd** command in interface configuration mode with the **disable** keyword to disable BFD for a specific OSPF interface.

Examples

In the following example, the interface associated with OSPF, Fast Ethernet interface 3/0, is configured for BFD:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# ip ospf bfd
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.

isis bfd

To enable or disable Bidirectional Forwarding Detection (BFD) on a specific interface configured for Intermediate System-to-Intermediate System (IS-IS), use the **isis bfd** command in interface configuration mode. To disable BFD on the IS-IS interface, use the **disable** keyword. To remove the **isis bfd** command, use the **no** form of this command.

isis bfd [**disable**]

no isis bfd

Syntax Description

disable	(Optional) Disables BFD for IS-IS on a specified interface.

Defaults

When the **disable** keyword is not used, the default behavior is to enable BFD support for IS-IS on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Enter the **isis bfd** command in interface mode to configure an IS-IS interface to use BFD for failure detection. If you have used the **bfd-all interfaces** command in router configuration mode to globally configure all IS-IS interfaces for an IS-IS process to use BFD, you can enter the **isis bfd** command with the **disable** keyword in interface configuration mode to disable BFD for a specific IS-IS interface.

Entering the **no isis bfd** command will remove the command. In that case, whether or not an IS-IS interface for a particular IS-IS process is registered with the BFD protocol will depend on whether or not you have entered the **bfd all-interfaces** command in router configuration mode for the specific IS-IS process.

Examples

In the following example, the interface associated with OSPF, Fast Ethernet interface 3/0, is configured for BFD:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# isis bfd
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.

show bfd neighbors

To display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies, use the **show bfd neighbors** command in user EXEC or privileged EXEC mode.

show bfd neighbors [**details**]

Syntax Description

details	(Optional) Displays BFD protocol parameters and timers for each neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

0S Release	Modification
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
S Release	**Modification**
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
T Release	**Modification**
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(9)T	Support for BFD Version 1 and BFD echo mode was added.

Usage Guidelines

The **show bfd neighbors** command can be used to help troubleshoot the BFD feature.

The full output for the **details** keyword is not supported on the Route Processor (RP) for the Cisco 12000 series Internet router. If you want to enter the **show bfd neighbors** command with the **details** keyword for the Cisco 12000 series Internet router, you must enter it on the line card. Use the **attach** *slot* command to establish a command-line interface (CLI) session with a line card.

Examples

Examples for 12.0(31)S, 12.2(18)SXE, 12.2(33)SRA, and 12.3(4)T

The following sample output shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors

OurAddr       NeighAddr      LD/RD RH  Holdown(mult) State     Int
172.16.10.1   172.16.10.2    1/6  1   260  (3 )      Up        Fa0/1
```

The following sample output from the **show bfd neighbors** command entered with the **details** keyword shows BFD protocol parameters and timers for each neighbor:

```
Router# show bfd neighbors details

OurAddr       NeighAddr      LD/RD RH  Holdown(mult) State     Int
172.16.10.1   172.16.10.2    1/2  1   460  (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(390169)
Rx Count: 229225, Rx Interval (ms) min/max/avg: 208/440/332 last: 144 ms ago
Tx Count: 388219, Tx Interval (ms) min/max/avg: 148/248/196 last: 48 ms ago
Registered protocols: OSPF Stub
Uptime: 17:44:37
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 following sample output from the RP on a Cisco 12000 series router shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/0  0   0    (0 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from the RP on a Cisco 12000 series router shows the status of the adjacency or neighbor with the **details** keyword:

```
RouterB# 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    2/0  0   0    (0 )      Up        Fa6/0
Registered protocols: OSPF
Uptime: never
%% BFD Neighbor statistics are not available on RP. Please execute this command on Line
Card.
```

The following sample output from a line card on a Cisco 12000 series router shows the status of the adjacency or neighbor:

```
Router# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session

Press RETURN to get started!

LC-Slot6> show bfd neighbors

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/1  1   848  (5 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from a line card on a Cisco 12000 series router shows the status of the adjacency or neighbor with the **details** keyword:

```
Router# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
```

```
Press RETURN to get started!

LC-Slot6> 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    2/1  1   892  (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(193745)
Rx Count: 327406, Rx Interval (ms) min/max/avg: 152/248/196 last: 108 ms ago
Tx Count: 193748, Tx Interval (ms) min/max/avg: 204/440/331 last: 408 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.: 2
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 17:54:07
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 7728507 min/max/avg: 8/16/8 last: 12 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
LC-Slot6>
```

Example for 12.4(9)T and Later Releases

The following sample output Sverifies that the BFD neighbor router is also running BFD Version 1 and that the BFD session is up and running in echo mode.

```
Router# 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        Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

Table 3 describes the significant fields shown in the display.

Table 3 show bfd neighbors Field Descriptions

Field	Description
OurAddr	IP address of the interface for which the **show bfd neighbors** command was entered.
NeighAddr	IP address of the BFD adjacency or neighbor.
LD/RD	Local discriminator and remote discriminator being used for the session.
RH	Remote Heard—Indicates that the remote BFD neighbor has been heard.
Holdown(mult)	The detect timer multiplier that is used for this session.
State	State of the interface—Up or Down.
Int	Interface type and slot/port.
Session state is UP and using echo function with 50 ms interval.	BFD is up and running in echo mode. The 50-millisecond interval has been adopted from the **bfd** command. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
RX Count	Number of BFD control packets that have been received from the BFD neighbor.
TX Count	Number of BFD control packets that have been sent by the BFD neighbor.
TX Interval	The interval between sent BFD packets.
Registered protocols	Routing protocols that have been registered with BFD.
Last packet: Version:	BFD version detected and run between the BFD neighbors. 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. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Diagnostic	A diagnostic code specifying the local system’s reason for the last transition of the session from Up to some other state. State values are as follows: • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down

Table 3 show bfd neighbors Field Descriptions (continued)

Field	Description
I Hear You bit	I Hear You Bit. This bit is set to 0 if the transmitting system either is not receiving BFD packets from the remote system or is tearing down the BFD session for some reason. During normal operation the I Hear You bit is set to 1 to signify that the remote system is receiving the BFD packets from the transmitting system.
Demand bit	Demand Mode bit. If set, the transmitting system wants to operate in demand mode. BFD has two modes—asynchronous and demand. The Cisco implementation of BFD supports only asynchronous mode.
Poll bit	Poll bit. If the Poll bit is set, the transmitting system is requesting verification of connectivity or of a parameter change.
Final Bit	Final bit. If the Final bit is set, the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.
Multiplier	Detect time multiplier. The negotiated transmit interval, multiplied by the detect time multiplier, determines the detection time for the transmitting system in BFD asynchronous mode. The detect time multiplier is similar to the hello multiplier in Intermediate System-to-Intermediate System (IS-IS), which is used to determine the hold timer: (hello interval) * (hello multiplier) = hold timer. If a hello packet is not received within the hold timer interval, a failure has occurred. Similarly, 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.
Length	Length of the BFD control packet, in bytes.
My Discr	My Discriminator. Unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discr	Your Discriminator. The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator, or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.
Min Echo interval	Minimum interval, in microseconds, between received BFD control packets that the system can support. If the value is zero, the transmitting system does not support the receipt of BFD echo packets. The Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE and 12.0(31)S does not support the use of echo packets.

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing monitoring and maintenance commands on that line card only.

show clns interface

To list the CLNS-specific information about each interface, use the **show clns interface** command in privileged EXEC mode.

show clns interface [*type number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.

Command Modes

Privileged EXEC

Command History

Mainline Release	Modification
10.0	This command was introduced.
0S Release	
12.0(31)S	Support for the BFD feature was added.
S Release	
12.2(18)SXE	Support for the Bidirectional Forwarding Detection (BFD) feature was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
T Release	
12.4(4)T	Support for the BFD feature was added.

Examples

The following is sample output from the **show clns interface** command that includes information for Token Ring and serial interfaces:

```
Router# show clns interface

TokenRing 0 is administratively down, line protocol is down
  CLNS protocol processing disabled
TokenRing 1 is up, line protocol is up
  Checksums enabled, MTU 4461, Encapsulation SNAP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
  Congestion Experienced bit set at 4 packets
  CLNS fast switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 18 seconds
  Routing Protocol: ISO IGRP
      Routing Domain/Area: <39.0003> <0020>
Serial 2 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation HDLC
ERPDUs enabled, min. interval 10 msec.
     RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
     Congestion Experienced bit set at 4 packets
     CLNS fast switching enabled
     DEC compatibility mode OFF for this interface
     CLNS cluster alias enabled on this interface
```

```
      Next ESH/ISH in 48 seconds
   Routing Protocol: IS-IS
        Circuit Type: level-1-2
        Level-1 Metric: 10, Priority: 64, Circuit ID: 0000.0C00.2D55.0A
        Number of active level-1 adjacencies: 0
        Level-2 Metric: 10, Priority: 64, Circuit ID: 0000.0000.0000.00
        Number of active level-2 adjacencies: 0
        Next IS-IS LAN Level-1 hello in 3 seconds
        Next IS-IS LAN Level-2 hello in 3 seconds
```

Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

The following is sample output from the **show clns interface** command that verifies that the BFD feature has been enabled on Ethernet interface 3/0. The relevant command output is shown in bold in the output.

```
Router# show clns interface ethernet 3/0

Ethernet3/0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 42 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x1, local circuit ID 0x2
    Level-1 Metric: 10, Priority: 64, Circuit ID: RouterA.02
    DR ID: 0000.0000.0000.00
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10, Priority: 64, Circuit ID: RouterA.02
    DR ID: 0000.0000.0000.00
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 3 seconds
    Next IS-IS LAN Level-2 Hello in 5 seconds
    BFD enabled
```

Table 4 describes the significant fields shown in the display.

Table 4 show clns interface Field Descriptions

Field	Description
TokenRing 0 is administratively down, line protocol is down	(First interface). Shown to be administratively down with CLNS disabled.
TokenRing 1 is up, line protocol is up	(Second interface). Shown to be up, and the line protocol is up.
Serial 2 is up, line protocol is up	(Third interface). Shown to be up, and the line protocol is up.
Checksums enabled	Can be enabled or disabled.
MTU	The number following maximum transmission unit (MTU) is the maximum transmission size for a packet on this interface.
Encapsulation	Describes the encapsulation used by CLNP packets on this interface.

Table 4 show clns interface Field Descriptions (continued)

Field	Description
ERPDUs	Displays information about the generation of error protocol data units (ERPDUs). They can be either enabled or disabled. If they are enabled, they are sent out no more frequently than the specified interval.
RDPDUs	Provides information about the generation of redirect protocol data units (RDPDUs). They can be either enabled or disabled. If they are enabled, they are sent out no more frequently than the specified interval. If the address mask is enabled, redirects are sent out with an address mask.
Congestion Experienced	Tells when CLNS will turn on the congestion experienced bit. The default is to turn this bit on when there are more than four packets in a queue.
CLNS fast switching	Displays whether fast switching is supported for CLNS on this interface.
DEC compatibility mode	Indicates whether Digital Equipment Corporation (DEC) compatibility has been enabled.
CLNS cluster alias enabled on this interface	Indicates that CLNS cluster aliasing has been enabled on this interface.
Next ESH/ISH	Displays when the next end system (ES) hello or intermediate system (IS) hello will be sent on this interface.
Routing Protocol	Lists the areas that this interface is in. In most cases, an interface will be in only one area.
Circuit Type	Indicates whether the interface has been configured for local routing (level 1), area routing (level 2), or local and area routing (level 1-2).
Interface number, local circuit ID Level-1 Metric DR ID Level-1 IPv6 Metric Number of active level-1 adjacencies Level-2 Metric DR ID Level-2 IPv6 Metric Number of active level-2 adjacencies Next IS-IS LAN Level-1 Next IS-IS LAN Level-2	Last series of fields displays information pertaining to the International Organization for Standardization (ISO) CLNS routing protocols enabled on the interface. For ISO Interior Gateway Routing Protocol (IGRP), the routing domain and area addresses are specified. For IS-IS, the Level 1 and Level 2 metrics, priorities, circuit IDs, and number of active Level 1 and Level 2 adjacencies are specified.
BFD enabled	BFD has been enabled on the interface.

show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

show ip bgp neighbors [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy** [**detail**]]]

Syntax Description

ip-address	(Optional) IP address of a neighbor. If this argument is omitted, all neighbors are displayed.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (external BGP peers only).
paths *reg-exp*	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
received prefix-filter	(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the **received-routes** keyword.
policy	(Optional) Displays the policies applied to this neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs) and AS-path filter lists.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **received-routes** keyword was added.
12.0(18)S	The output was modified to display the no-prepend configuration option and this command was integrated into Cisco IOS Release 12.0(18)S.
12.2(4)T	The **received** and **prefix-filter** keywords were added, and this command was integrated into Cisco IOS Release 12.2(4)T.
12.0(21)ST	The output was modified to display Multiprotocol Label Switching (MPLS) label information.

Release	Modification
12.0(22)S	Support for the BGP graceful restart capability was integrated into the output. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	Support for the BGP graceful restart capability was integrated into the output.
12.0(25)S	The **policy** and **detail** keywords were added.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.0(27)S	The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.3(7)T	The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.0(31)S	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.2(18)SXE	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(4)T	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the output was modified to support BGP TCP path MTU discovery.
12.4(11)T	Support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	Support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based the function or attribute that is displayed in the output.

Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, and Later Releases

When BGP neighbors use multiple levels of peer templates it can be difficult to determine which policies are applied to the neighbor. In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer-group or a peer-policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. To view the appropriate output, choose one of the following sections:

- show ip bgp neighbors: Example, page 75
- show ip bgp neighbors advertised-routes: Example, page 81
- show ip bgp neighbors paths: Example, page 82
- show ip bgp neighbors received prefix-filter: Example, page 82
- show ip bgp neighbors policy: Example, page 83
- Cisco IOS Release 12.0(31)S and 12.4(4)T: Example, page 83
- Cisco IOS Release 12.2(33)SRA: Example, page 83

show ip bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Router# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability:advertised and received
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          0
    Prefixes Total:                 0          0
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          0
    Used as multipath:            n/a          0

                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

Table 5 describes the significant fields shown in the display. Fields that are preceded by the asterisk character are displayed only when the counter has a nonzero value.

Table 5 show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous-system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when migrating autonomous systems.
internal link	“internal link” is displayed for iBGP neighbors. “external link” is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hhmmss, that the underlying TCP connection has been in existence.
Last read	Time, in hhmmss, since BGP last received a message from this neighbor.

Table 5 show ip bgp neighbors Field Descriptions (continued)

Field	Description
last write	Time, in hhmmss, since BGP last sent a message to this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
keepalive interval	Time, interval in seconds, that keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. “advertised and received” is displayed when a capability is successfully exchanged between two routers.
Route Refresh	Status of the route refresh capability.
MPLS Label Capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Received	Total number of received messages.
Opens	Number of open messages sent and received.
notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
For address family:	Address family for which the following fields refer.
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
...update-group	Number of update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes current	Number of prefixes accepted for this address family.
Prefixes total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.

Table 5 show ip bgp neighbors Field Descriptions (continued)

Field	Description
Explicit Withdraw	Number of times that prefix is withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as a best paths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS-path length policy denials.
* AS_PATH loop	Displays outbound AS-path loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of AS 0.
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound non-local next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress-map.
* advertise-map	Displays inbound denials due to an advertise-map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the bestpath came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Deploys inbound denials because the bestpath came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a CE router.

Table 5 show ip bgp neighbors Field Descriptions (continued)

Field	Description
* BGP distribute-list	Displays inbound denials due to a distribute list.
Number of NLRIs...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection have been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be... (not shown in the display)	Indicates that the BGP TTL security check is enabled. The maximum number hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgement hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keep alive packets.
GiveUp	Number times a packet is dropped due to no acknowledgement.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.

Table 5 show ip bgp neighbors Field Descriptions (continued)

Field	Description
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
with data	Number of update packets sent with data.
total data bytes	Total received in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
out of order:	Number of packets received out of sequence.
with data	Number of update packets received with data.
Last reset	Elapsed time since this peering session was last reset.
unread input bytes	Number of bytes of packets still to be processed.
retransmit	Number of packets retransmitted.
fastretransmit	A duplicate acknowledgement is retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgements (transmissions before or without subsequent acknowledgements).
Second Congestion	Second retransmission due to congestion.

show ip bgp neighbors advertised-routes: Example

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Router# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     0.0.0.0                0         32768 i
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.

Table 6 show ip bgp neighbors advertised-routes Field Descriptions (continued)

Field	Description
Metric	If shown, this is the value of the inter-autonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp neighbors paths: Example

The following is example output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Router# show ip bgp neighbors 172.29.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

show ip bgp neighbors received prefix-filter: Example

The following example shows that a prefix-list the filters all routes in the 10.0.0.0 network has be received from the 192.168.20.72 neighbor:

```
Router# show ip bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

show ip bgp neighbors policy: Example

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited polices are policies that the neighbor inherits from a peer-group or a peer-policy template.

```
Router# show ip bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

Cisco IOS Release 12.0(31)S and 12.4(4)T: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that BFD is being used to detect fast fallover for the BGP neighbor that is a BFD peer.

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
.
.
.
 Using BFD to detect fast fallover
```

Cisco IOS Release 12.2(33)SRA: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path MTU discovery is enabled for the BGP neighbor at 172.16.1.2.

```
Router# show ip bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

Related Commands

Command	Description
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.

show ip eigrp interfaces

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ip eigrp interfaces** command in privileged EXEC mode.

show ip eigrp interfaces [*type number*] [*as-number*] [**detail**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
as-number	(Optional) Autonomous system number.
detail	(Optional) Displays detailed information about the EIGRP interfaces for a specific EIGRP process.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(18)SXE	Support for the Bidirectional Forwarding Detection (BFD) feature was added. The **detail** keyword was added.
12.0(31)S	The BFD feature was integrated into Cisco IOS Release 12.0(31)S. Support was added for the Cisco 12000 series Internet router.
12.4(4)T	Support for the BFD feature was added. The **detail** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show ip eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

The following is sample output from the **show ip eigrp interfaces** command:

```
Router# show ip eigrp interfaces

IP EIGRP interfaces for process 109

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Di0           0         0/0         0       11/434          0          0
Et0           1         0/0       337        0/10           0          0
SE0:1.16      1         0/0        10        1/63         103          0
Tu0           1         0/0       330        0/16           0          0
```

Cisco IOS Release 12.2(18)SXE

The following is sample output from the **show ip eigrp interfaces** command to verify that the BFD feature has been enabled on the EIGRP interfaces for process 123. The relevant command output is shown in bold in the output.

```
Router# show ip eigrp interfaces detail

IP-EIGRP interfaces for process 1

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
IP-EIGRP interfaces for process 100

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT  Un/Reliable  Flow Timer    Routes
Fa0/1              0        0/0        0       0/10            0           0
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is not set
   BFD is enabled
Et3/0               0        0/0       0        0/10           0            0
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is not set
  BFD is enabled
```

Table 9 describes the significant fields shown in the display.

Table 9 show ip eigrp interfaces Field Descriptions

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time (SRTT) interval (in seconds).
Pacing Time Un/Reliable	Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the router will send multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.
BFD is enabled	Confirmation that BFD is enabled on this interface.

Related Commands

Command	Description
show ip eigrp vrf neighbors	Displays the neighbors discovered by EIGRP.

show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ip ospf** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*]

Syntax Description

process-id	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.

Command Modes

User EXEC
Privileged EXEC

Command History

Mainline Release	Modification
10.0	This command was introduced.
0S Release	**Modification**
12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)S and the output was expanded to display link-state advertisement (LSA) throttling timers.
12.0(31)S	Support for the BFD feature was added.
S Release	**Modification**
12.2(14)S	Support for displaying packet pacing timers was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and support for the Bidirectional Forwarding Detection (BFD) feature was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
T Release	**Modification**
12.2(4)T	This command was modified to show packet pacing timers in the displayed output.
12.2(15)T	This command was modified to show additional information if the OSPF Forwarding Address Suppression in Type-5 LSAs feature is configured.
12.3(2)T	The output of this command was expanded to display LSA throttling timers and the limit on redistributed routes.
12.4(4)T	Support for the BFD feature was added.

Examples

The following is sample output from the **show ip ospf** command when entered without a specific OSPF process ID:

```
Router# show ip ospf

  Routing Process "ospf 201" with ID 10.0.0.1 and Domain ID 10.20.0.1
  Supports only single TOS(TOS0) routes
```

```
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 100 secs
 Interface flood pacing timer 55 msecs
 Retransmission pacing timer 100 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 2. 2 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has message digest authentication
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x29BEB
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 3
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 172.16.26.0
        Number of interfaces in this area is 0
        Area has no authentication
        SPF algorithm executed 1 times
        Area ranges are
           192.168.0.0/16 Passive Advertise
        Number of LSA 1. Checksum Sum 0x44FD
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 1
        Number of indication LSA 1
        Number of DoNotAge LSA 0
        Flood list length 0
```

Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

The following is sample output from the **show ip ospf** command to verify that the BFD feature has been enabled for OSPF process 123. The relevant command output is shown in bold in the output.

```
Router# 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
        Area has no authentication
        SPF algorithm last executed 00:00:03.708 ago
        SPF algorithm executed 27 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x00AEF1
        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
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip ospf Field Descriptions

Field	Description
Routing process "ospf 201" with ID 10.0.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
SPF schedule delay	Delay time of SPF calculations.
Minimum LSA interval	Minimum interval between link-state advertisements.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.
Number of areas in this router is	Number of areas configured for the router.
External flood list length	External flood list length.
BFD is enabled	BFD has been enabled on the OSPF process.

The following is an excerpt of output from the **show ip ospf** command when the OSPF Forwarding Address Suppression in Type-5 LSAs feature is configured:

```
Router# show ip ospf
.
.
.
Area 2
   Number of interfaces in this area is 4
   It is a NSSA area
   Perform type-7/type-5 LSA translation, suppress forwarding address
.
.
.
Routing Process "ospf 1" with ID 192.168.0.1
 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 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 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip ospf Field Descriptions

Field	Description
Area	OSPF area and tag.
Number of interfaces...	Number of interfaces configured in the area.
It is...	Possible types are internal, area border, or autonomous system boundary.
Routing process “ospf 1” with ID 192.168.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
Initial SPF schedule delay	Delay time of SPF calculations at startup.
Minimum hold time	Minimum hold time between consecutive SPF calculations.
Maximum wait time	Maximum wait time between consecutive SPF calculations.
Incremental-SPF	Status of incremental SPF calculations.
Minimum LSA...	Minimum time interval (in seconds) between link-state advertisements, and maximum arrival time (in milliseconds) of link-state advertisements,
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of...	Number and type of link-state advertisements that have been received.
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.

Table 11 show ip ospf Field Descriptions (continued)

Field	Description
Number of areas in this router is	Number of areas configured for the router listed by type.
External flood list length	External flood list length.

The following is sample output from the **show ip ospf** command. In this example, the user had configured the **redistribution maximum-prefix** command to set a limit of 2000 redistributed routes. Shortest Path First (SPF) throttling was configured with the **timers throttle spf** command.

```
Router# show ip ospf 1

 Routing Process "ospf 1" with ID 10.0.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
    Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip ospf Field Descriptions

Field	Description
Routing process “ospf 1” with ID 10.0.0.1	Process ID and OSPF router ID.
Supports ...	Number of Types of Service (TOS) supported.
It is ...	Possible types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum limit of redistributed prefixes	Value set in the **redistribution maximum-prefix** command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the **redistribution maximum-prefix** command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.
Initial SPF schedule delay	Delay (in milliseconds) before initial SPF schedule for SPF throttling. Configured with the **timers throttle spf** command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **show ip ospf** command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```
Router# show ip ospf 1

Routing Process "ospf 4" with ID 10.10.24.4
 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
 Initial LSA throttle delay 100 msecs
 Minimum hold time for LSA throttle 10000 msecs
 Maximum wait time for LSA throttle 45000 msecs
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
 External flood list length 0
    Area 24
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 04:28:18.396 ago
        SPF algorithm executed 8 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x23EB9
        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 following is sample **show ip ospf** command. In this example, the user had configured the **redistribution maximum-prefix** command to set a limit of 2000 redistributed routes. SPF throttling was configured with the **timers throttle spf** command.

```
Router# show ip ospf 1

 Routing Process "ospf 1" with ID 192.168.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
    Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
```

Table 13 describes the significant fields shown in the display.

Table 13 show ip ospf Field Descriptions

Field	Description
Routing process "ospf 1" with ID 192.168.0.0.	Process ID and OSPF router ID.
Supports ...	Number of TOS supported.
It is ...	Possible types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum limit of redistributed prefixes	Value set in the **redistribution maximum-prefix** command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the **redistribution maximum-prefix** command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.
Initial SPF schedule delay	Delay (in milliseconds) before the initial SPF schedule for SPF throttling. Configured with the **timers throttle spf** command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **show ip ospf** command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```
Router# show ip ospf 1

Routing Process "ospf 4" with ID 10.10.24.4
 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
 Initial LSA throttle delay 100 msecs
 Minimum hold time for LSA throttle 10000 msecs
 Maximum wait time for LSA throttle 45000 msecs
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
 External flood list length 0
    Area 24
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 04:28:18.396 ago
        SPF algorithm executed 8 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x23EB9
        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
```

show monitor event-trace

To display event trace messages for Cisco IOS software subsystem components, use the **show monitor event-trace** command in privileged EXEC mode.

show monitor event-trace [**all-traces**] [*component* {**all** | **back** *time* | **clock** *time* | **from-boot** *seconds* | **latest** | **parameters**}]

Syntax Description

all-traces	(Optional) Displays all event trace messages in memory to the console.
component	(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the **monitor event-trace ?** command.
all	Displays all event trace messages currently in memory for the specified component.
back *time*	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes. The time argument is specified in hours and minutes format (hh:mm).
clock *time*	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
from-boot *seconds*	Displays event trace messages starting from a specified number of seconds after booting (uptime). To view the uptime, in seconds, enter the **show monitor event-trace** *component* **from-boot ?** command.
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
parameters	Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. The **spa** component keyword was added to support OIR event messages for shared port adapters (SPAs). The **bfd** keyword was added as a possible entry for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.
12.4(4)T	Support for the **bfd** keyword was implemented in Cisco IOS Release 12.4(4)T.
12.0(31)S	Support for the **bfd** keyword was implemented in Cisco IOS Release 12.0(31)S.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.4(9)T	The **cfd** keyword was added as a possible entry for the *component* argument to display trace messages relating to crypto fault detection.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information.

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace** command will generate a message indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace** command will stop displaying messages.

Use the **bfd** keyword for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.

Use the **cfd** keyword for the *component* argument to display trace messages relating to the crypto fault detection feature. This keyword displays the contents of the error trace buffers in an encryption data path.

Examples

IPC Component Example

The following is sample output from the **show monitor event-trace** *component* command for the IPC component. Notice that each trace message is numbered and is followed by a timestamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace ipc

3667:  6840.016:Message type:3 Data=0123456789
3668:  6840.016:Message type:4 Data=0123456789
3669:  6841.016:Message type:5 Data=0123456789
3670:  6841.016:Message type:6 Data=0123456
```

BFD Component for Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

Use the **show monitor event-trace bfd all** command to display logged messages for important BFD events in the recent past. The following trace messages show BFD session state changes:

```
Router# show monitor event-trace bfd all

    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], event Session
           create, state Unknown -> Fail
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Fail -> Down
            (from LC)
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Down -> Init
            (from LC)
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Init -> Up
           (from LC)
    3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], event Session
           create, state Unknown -> Fail
```

```
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Fail -> Down
              (from LC)
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Down -> Up
             (from LC)
```

To view trace information for all components configured for event tracing on the networking device, enter the **show monitor event-trace all-traces** command. In this example, separate output is provided for each event, and message numbers are interleaved between the events.

```
Router# show monitor event-trace all-traces

Test1 event trace:
3667: 6840.016:Message type:3 Data=0123456789
3669: 6841.016:Message type:4 Data=0123456789
3671: 6842.016:Message type:5 Data=0123456789
3673: 6843.016:Message type:6 Data=0123456789

Test2 event trace:
3668: 6840.016:Message type:3 Data=0123456789
3670: 6841.016:Message type:4 Data=0123456789
3672: 6842.016:Message type:5 Data=0123456789
3674: 6843.016:Message type:6 Data=0123456789
```

SPA Component Example

The following is sample output from the **show monitor event-trace** *component* **latest** command for the **spa** component:

```
Router# show monitor event-trace spa latest

00:01:15.364: subslot 2/3: 4xOC3 POS SPA, TSM Event:inserted  New state:wait_psm
_ready
     spa type 0x440
00:02:02.308: subslot 2/0: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/0: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/1: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/2: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete  New state:idle
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty  New
state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete  New state:idle
```

Cisco Express Forwarding Component Examples

If you select Cisco Express Forwarding as the component for which to display event messages, you can use the following additional arguments and keywords: **show monitor event-trace cef** [**events** | **interface** | **ipv6** | **ipv4**][**all**].

The following example shows the IPv6 or IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv6 all

00:00:24.612:  [Default] *::*/*'00             New FIB table          [OK]

Router# show monitor event-trace cef ipv4 all

00:00:24.244:  [Default] 127.0.0.81/32'01       FIB insert             [OK]
```

In the following example, all event trace messages for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all

00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.612: SubSys  ipv6fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following example shows Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet0/1(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Cisco Express Forwarding Component Examples for Cisco 10000 Series Routers Only

The following example shows the IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a the time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv4 all

00:00:48.244:  [Default] 127.0.0.81/32'01      FIB insert               [OK]
```

In the following example, all event trace message for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all

00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
```

```
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following examples show Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet1/0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet1/0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet1/1/0(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

CFD Component for Cisco IOS Release 12.4(9)T

To troubleshoot errors in an encryption datapath, enter the **show monitor event-trace cfd all** command. In this example, events are shown separately, each beginning with a timestamp, followed by data from the error trace buffer. Cisco TAC engineers can use this information to diagnose the cause of the errors.

Note If no packets have been dropped, this command does not display any output.

```
Router# show monitor event-trace cfd all

00:00:42.452: 450000B4 00060000 FF33B306 02020203 02020204 32040000 F672999C
        00000001 7A7690C2 A0A4F8BC E732985C D6FFDCC8 00000001 C0902BD0
        A99127AE 8EAA22D4

00:00:44.452: 450000B4 00070000 FF33B305 02020203 02020204 32040000 F672999C
        00000002 93C01218 2325B697 3C384CF1 D6FFDCC8 00000002 BFA13E8A
        D21053ED 0F62AB0E

00:00:46.452: 450000B4 00080000 FF33B304 02020203 02020204 32040000 F672999C
        00000003 7D2E11B7 A0BA4110 CC62F91E D6FFDCC8 00000003 7236B930
        3240CA8C 9EBB44FF

00:00:48.452: 450000B4 00090000 FF33B303 02020203 02020204 32040000 F672999C
        00000004 FB6C80D9 1AADF938 CDE57ABA D6FFDCC8 00000004 E10D8028
        6BBD748F 87F5E253

00:00:50.452: 450000B4 000A0000 FF33B302 02020203 02020204 32040000 F672999C
        00000005 697C8D9D 35A8799A 2A67E97B D6FFDCC8 00000005 BC21669D
        98B29FFF F32670F6

00:00:52.452: 450000B4 000B0000 FF33B301 02020203 02020204 32040000 F672999C
        00000006 CA18CBC4 0F387FE0 9095C27C D6FFDCC8 00000006 87A54811
        AE3A0517 F8AC4E64
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [*type number* [*group*]] [**all** | **brief**]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.
group	(Optional) Group number on the interface for which output is displayed.
all	(Optional) Displays information for groups that are learned or do not have the **standby ip** command configured.
brief	(Optional) A single line of output summarizes each standby group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The output for the command was made clearer and easier to understand.
12.3(2)T	The output was enhanced to display information about Message Digest 5 (MD5) authentication.
12.3(4)T	The output was enhanced to display information about HSRP version 2.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	IPv6 support was added.
12.4(6)T	The output for this command was enhanced to display information about HSRP master and client groups.
12.4(9)T	The output for this command was enhanced to display information about HSRP group shutdown configuration.
12.4(11)T	The output for this command was enhanced to display information about HSRP Bidirectional Forwarding Detection (BFD) peering.

Usage Guidelines

To specify a group, you must specify an interface type and number.

Examples

The following is sample output from the **show standby** command:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
```

```
    Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
IP redundancy name is “HSRP1” (cfgd)
Follow by groups:
    Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.666)
    Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.491)
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
  IP redundancy name is "HSRP1", advertisement interval is 34 sec
```

The following is sample output from the **show standby** command when HSRP version 2 is configured:

```
Router# show standby

Ethernet0/1 - Group 1 (version 2)
  State is Speak
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is unknown
   Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
   Next hello sent in 1.804 secs
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 20 (configured 20)
  IP redundancy name is "hsrp-Et0/1-1" (default)

Ethernet0/2 - Group 1
  State is Speak
  Virtual IP address is 10.22.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (default 100)
    Track interface Serial2/0 state Down decrement 10
  IP redundancy name is "hsrp-Et0/2-1" (default)
```

The following is sample output from the **show standby** command with the **brief** keyword specified:

```
Router# show standby brief

Interface   Grp Prio P State    Active addr     Standby addr    Group addr
Et0         0   120    Init     10.0.0.1        unknown         10.0.0.12
```

The following is sample output from the **show standby** command when HSRP MD5 authentication is configured:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
```

```
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string "f33r45", timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Et0/1-1" (default)
```

The following is sample output from the **show standby** command when HSRP group shutdown is configured:

```
Router# show standby

Ethernet0/0 - Group 1
State is Init (tracking shutdown)
3 state changes, last state change 00:30:59
Track object 100 state Up
Track object 101 state Down
Track object 103 state Up
```

The following is sample output from the **show standby** command when HSRP BFD peering is enabled:

```
Router# show standby

Ethernet0/0 - Group 2
  State is Listen
    2 state changes, last state change 01:18:18
  Virtual IP address is 10.0.0.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is 10.0.0.250, priority 120 (expires in 9.396 sec)
  Standby router is 10.0.0.251, priority 110 (expires in 8.672 sec)
    BFD enabled
  Priority 90 (configured 90)
  IP redundancy name is "hsrp-Et0/0-1" (default)
```

Table 14 describes the significant fields shown in the displays.

Table 14 show standby Field Descriptions

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface.
State is	State of local router; can be one of the following: • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active addr and Standby addr fields will show "unknown." The state is listed as disabled in the fields when the **standby ip** command has not been specified. • Init (tracking shutdown)—HSRP groups appear in the Init state when HSRP group shutdown has been configured and a tracked object goes down.
Virtual IP address is, Secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as "duplicate." A duplicate address indicates that the router has failed to defend its ARP (Address Resolution Protocol) cache entry.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Local virtual MAC address	Virtual MAC address that would be used if this router became the active router. The origin of this address (displayed in parentheses) can be "default," "bia," (burned-in address) or "confgd" (configured).
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the command. The holdtime is the time (in seconds) before other routers declare the active or standby router to be down, based on the **standby timers** command. All routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
Next hello sent in	Time in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Authentication	Authentication type configured based on the **standby authentication** command.
key-string	Key string used for authentication. Key chains are displayed if configured.
timeout	Duration (in seconds) that HSRP will accept message digests based on both the old and new keys.
Preemption enabled, sync delay	Indicates whether preemption is enabled. If enabled, the minimum delay is the time a higher-priority nonactive router will wait before preempting the lower-priority active router. The sync delay is the maximum time a group will wait to synchronize with the IP redundancy clients.

Table 14 show standby Field Descriptions (continued)

Field	Description
Active router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the current active Hot Standby router.
Standby router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the “standby” router (the router that is next in line to be the Hot Standby router).
BFD enabled	Indicates that BFD peering is enabled on the router.
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Tracking	List of interfaces that are being tracked and their corresponding states. Based on the **standby track** command.
IP redundancy name is	The name of the HSRP group.
Follow by groups:	Indicates the client HSRP groups that have been configured to follow this HSRP group.
P	Indicates that the router is configured to preempt.

Related Commands

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby mac-address	Specifies the virtual MAC address for the virtual router.
standby mac-refresh	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
standby timers	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bias	Configures HSRP to use the BIA of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

show standby neighbors

To display information about Hot Standby Router Protocol (HSRP) peer routers on an interface, use the **show standby neighbors** command in privileged EXEC mode.

show standby neighbors [interface-*type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number for which output is displayed.

Command Default

HSRP neighbor information is displayed for all interfaces.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display information about HSRP peer neighbors. This command displays the HSRP groups for which each neighbor is acting as the active and standby router and whether Bidirectional Forwarding Detection (BFD) peering is enabled for each neighbor.

Examples

The following example displays the HSRP neighbors on Ethernet interface 0/0. Neighbor 10.0.0.250 is active for group 2 and standby for groups 1 and 8, and is registered with BFD:

```
Router# show standby neighbors Ethernet0/0

HSRP neighbors on Ethernet0/0
  10.0.0.250
    Active groups: 2
    Standby groups: 1, 8
    BFD enabled
  10.0.0.251
    Active groups: 5, 8
    Standby groups: 2
    BFD enabled
  10.0.0.253
    No Active groups
    No Standby groups
    BFD enabled
```

The following example displays information for all HSRP neighbors:

```
Router# show standby neighbors

HSRP neighbors on FastEthernet2/0
  10.0.0.2
    No active groups
    Standby groups: 1
    BFD enabled

HSRP neighbors on FastEthernet2/0
  10.0.0.1
    Active groups: 1
    No standby groups
    BFD enabled
```

Table 15 describes the significant fields shown in the displays.

Table 15 show standby neighbors Field Descriptions

Field	Description
Active groups	HSRP groups for which an interface is acting as the active peer.
Standby groups	HSRP groups for which an interface is acting as the standby peer.
BFD enabled	Indicates that HSRP BFD peering is enabled.

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
debug standby events neighbor	Displays HSRP neighbor events.
show bfd neighbor	Displays a line-by-line listing of existing BFD adjacencies.
show standby	Displays information about HSRP.
standby bfd	Reenables HSRP BFD peering for a specified interface if it has been disabled.
standby ip	Activates HSRP.

standby bfd

To reenable Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering if it has been disabled on an interface, use the **standby bfd** command in interface configuration mode. To disable HSRP support for BFD, use the **no** form of this command.

standby bfd

no standby bfd

Syntax Description

This command has no arguments or keywords.

Command Default

HSRP support for BFD is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

HSRP BFD peering is enabled by default when the router is configured for BFD. Use this command to reenable HSRP BFD peering on the specified interface when it has previously been manually disabled.

To enable HSRP BFD peering globally on the router, use the **standby bfd all-interfaces** command in global configuration mode.

Examples

The following example shows how to reenable HSRP BFD peering if it has been disabled:

```
Router(config)# interface ethernet0/0
Router(config-if)# standby bfd
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
debug standby events neighbor	Displays HSRP neighbor events.
show bfd neighbor	Displays a line-by-line listing of existing BFD adjacencies.
show standby	Displays HSRP information.
show standby neighbors	Displays information about HSRP neighbors.
standby bfd all-interfaces	Reenables HSRP BFD peering on all interfaces if it has been disabled.
standby ip	Activates HSRP.

standby bfd all-interfaces

To reenable Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering on all interfaces if it has been disabled, use the **standby bfd all-interfaces** command in global configuration mode. To disable HSRP support for BFD peering, use the **no** form of this command.

standby bfd all-interfaces

no standby bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

HSRP BFD peering is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The HSRP BFD peering feature introduces BFD in the HSRP group member health monitoring system. Previously, group member monitoring relied exclusively on HSRP multicast messages, which are relatively large and consume CPU memory to produce and check. In architectures where a single interface hosts a large number of groups, there is a need for a protocol with low CPU memory consumption and processing overhead. BFD addresses this issue and offers subsecond health monitoring (failure detection in milliseconds) with a relatively low CPU impact. This command is enabled by default.

To enable HSRP support for BFD on a per-interface basis, use the **standby bfd** command in interface configuration mode.

Examples

The following example shows how to reenable HSRP BFD peering if it has been disabled on a router:

```
Router(config)# standby bfd all-interfaces
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
debug standby events neighbor	Displays HSRP neighbor events.
show bfd neighbor	Displays a line-by-line listing of existing BFD adjacencies.
show standby	Displays information about HSRP.

Command	Description
show standby neighbors	Displays information about HSRP neighbors.
standby bfd	Reenables HSRP BFD peering for a specified interface if it has been disabled.
standby ip	Activates HSRP.

Feature Information for Bidirectional Forwarding Detection

Table 16 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 16 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 16 Feature Information for Bidirectional Forwarding Detection

Feature Name	Releases	Feature Information
Bidirectional Forwarding Detection	12.2(18)SXE 12.0(31)S 12.4(4)T 12.0(32)S 12.2(33)SRA 12.4(9)T 12.4(11)T 12.2(33)SRB	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. In Release 12.0(31)S, support was added for the Cisco 12000 series Internet router. In Release 12.0(32)S, support was added for the Cisco 10720 Internet router and IP Services Engine (Engine 3) and Engine 5 shared port adapters (SPAs) and SPA interface processors (SIPs) on the Cisco 12000 series Internet router. In Release 12.4(9)T, support for Version 1 BFD and support for BFD Echo Mode was added. 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. In Release 12.4(11)T, support for HSRP was added. In Release 12.2(33)SRB, BFD standard implementation, Version 1, and echo mode is supported on the Cisco 7600 router in Cisco IOS Release 12.2(33)SRB.

Glossary

BFD—Bidirectional Forwarding Detection. A detection protocol designed to provide fast failure detection times for all media types, encapsulations, topologies, and routing protocols.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.