



## **Cisco IOS IP Routing: BFD Configuration Guide**

Release 15.0

### **Americas Headquarters**

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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.

*Cisco IOS IP Routing: BFD Configuration Guide*  
© 2008 Cisco Systems, Inc. All rights reserved.



# About Cisco IOS Software Documentation

---

**Last Updated: October 14, 2009**

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page i](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xii](#)

## Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

## Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

## Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section contains the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

## Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

## Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
<b>bold</b>	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y   z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

## Software Conventions

Cisco IOS software uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
<b>Courier font</b>	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

## Reader Alert Conventions

Cisco IOS documentation uses the following conventions for reader alerts:



**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

## Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

## Cisco IOS Documentation Set

The Cisco IOS documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

## Cisco IOS Documentation on Cisco.com

The following sections describe the organization of the Cisco IOS documentation set and how to access various document types.

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.

### New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

### Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

### Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

### Command References

Command reference books contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

### Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xi](#).

## Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references contain commands for Cisco IOS software for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

<http://www.cisco.com/go/techdocs>

**Table 1** *Cisco IOS Configuration Guides and Command References*

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk Command Reference</i></li> </ul>	AppleTalk protocol.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i></li> <li>• <i>Cisco IOS Asynchronous Transfer Mode Command Reference</i></li> </ul>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

**Table 1 Cisco IOS Configuration Guides and Command References (continued)**

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Bridging Command Reference</i></li> <li>• <i>Cisco IOS IBM Networking Command Reference</i></li> </ul>	<p>Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).</p> <p>Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Broadband Access Aggregation and DSL Configuration Guide</i></li> <li>• <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i></li> </ul>	<p>PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Carrier Ethernet Configuration Guide</i></li> <li>• <i>Cisco IOS Carrier Ethernet Command Reference</i></li> </ul>	<p>Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and Operation, Administration, and Maintenance (OAM).</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	<p>Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS DECnet Configuration Guide</i></li> <li>• <i>Cisco IOS DECnet Command Reference</i></li> </ul>	<p>DECnet protocol.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Technologies Configuration Guide</i></li> <li>• <i>Cisco IOS Dial Technologies Command Reference</i></li> </ul>	<p>Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Flexible NetFlow Configuration Guide</i></li> <li>• <i>Cisco IOS Flexible NetFlow Command Reference</i></li> </ul>	<p>Flexible NetFlow.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS High Availability Configuration Guide</i></li> <li>• <i>Cisco IOS High Availability Command Reference</i></li> </ul>	<p>A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Integrated Session Border Controller Command Reference</i></li> </ul>	<p>A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).</p>

**Table 1 Cisco IOS Configuration Guides and Command References (continued)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Intelligent Services Gateway Configuration Guide</i></li> <li>• <i>Cisco IOS Intelligent Services Gateway Command Reference</i></li> </ul>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface and Hardware Component Configuration Guide</i></li> <li>• <i>Cisco IOS Interface and Hardware Component Command Reference</i></li> </ul>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Addressing Services Configuration Guide</i></li> <li>• <i>Cisco IOS IP Addressing Services Command Reference</i></li> </ul>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Application Services Configuration Guide</i></li> <li>• <i>Cisco IOS IP Application Services Command Reference</i></li> </ul>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Mobility Configuration Guide</i></li> <li>• <i>Cisco IOS IP Mobility Command Reference</i></li> </ul>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Multicast Configuration Guide</i></li> <li>• <i>Cisco IOS IP Multicast Command Reference</i></li> </ul>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Routing Protocols Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing Protocols Command Reference</i></li> </ul>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), On-Demand Routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Routing: BFD Configuration Guide</i></li> </ul>	Bidirectional forwarding detection (BFD).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Routing: BGP Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: BGP Command Reference</i></li> </ul>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Routing: EIGRP Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: EIGRP Command Reference</i></li> </ul>	Enhanced Interior Gateway Routing Protocol (EIGRP).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Routing: ISIS Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: ISIS Command Reference</i></li> </ul>	Intermediate System-to-Intermediate System (IS-IS).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Routing: ODR Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: ODR Command Reference</i></li> </ul>	On-Demand Routing (ODR).

**Table 1 Cisco IOS Configuration Guides and Command References (continued)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: OSPF Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: OSPF Command Reference</i></li> </ul>	Open Shortest Path First (OSPF).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: Protocol-Independent Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i></li> </ul>	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: RIP Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: RIP Command Reference</i></li> </ul>	Routing Information Protocol (RIP).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP SLAs Configuration Guide</i></li> <li><i>Cisco IOS IP SLAs Command Reference</i></li> </ul>	Cisco IOS IP Service Level Agreements (IP SLAs).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Switching Configuration Guide</i></li> <li><i>Cisco IOS IP Switching Command Reference</i></li> </ul>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<ul style="list-style-type: none"> <li><i>Cisco IOS IPv6 Configuration Guide</i></li> <li><i>Cisco IOS IPv6 Command Reference</i></li> </ul>	For IPv6 features, protocols, and technologies, go to the IPv6 <a href="#">“Start Here”</a> document.
<ul style="list-style-type: none"> <li><i>Cisco IOS ISO CLNS Configuration Guide</i></li> <li><i>Cisco IOS ISO CLNS Command Reference</i></li> </ul>	ISO Connectionless Network Service (CLNS).
<ul style="list-style-type: none"> <li><i>Cisco IOS LAN Switching Configuration Guide</i></li> <li><i>Cisco IOS LAN Switching Command Reference</i></li> </ul>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i></li> </ul>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Home Agent Command Reference</i></li> </ul>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i></li> </ul>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i></li> </ul>	Cisco IOS radio access network products.
<ul style="list-style-type: none"> <li><i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i></li> <li><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></li> </ul>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.

**Table 1 Cisco IOS Configuration Guides and Command References (continued)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Multi-Topology Routing Configuration Guide</i></li> <li>• <i>Cisco IOS Multi-Topology Routing Command Reference</i></li> </ul>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS NetFlow Configuration Guide</i></li> <li>• <i>Cisco IOS NetFlow Command Reference</i></li> </ul>	Network traffic data analysis, aggregation caches, and export features.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Network Management Configuration Guide</i></li> <li>• <i>Cisco IOS Network Management Command Reference</i></li> </ul>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS Novell IPX Command Reference</i></li> </ul>	Novell Internetwork Packet Exchange (IPX) protocol.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Optimized Edge Routing Configuration Guide</i></li> <li>• <i>Cisco IOS Optimized Edge Routing Command Reference</i></li> </ul>	Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Securing the Data Plane</i></li> </ul>	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Securing the Control Plane</i></li> </ul>	Control Plane Policing, Neighborhood Router Authentication.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Securing User Services</i></li> </ul>	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.

**Table 1 Cisco IOS Configuration Guides and Command References (continued)**

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i></li> </ul>	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Service Advertisement Framework Configuration Guide</i></li> <li>• <i>Cisco IOS Service Advertisement Framework Command Reference</i></li> </ul>	Cisco Service Advertisement Framework.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Service Selection Gateway Configuration Guide</i></li> <li>• <i>Cisco IOS Service Selection Gateway Command Reference</i></li> </ul>	Subscriber authentication, service access, and accounting.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Activation Configuration Guide</i></li> <li>• <i>Cisco IOS Software Activation Command Reference</i></li> </ul>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Modularity Installation and Configuration Guide</i></li> <li>• <i>Cisco IOS Software Modularity Command Reference</i></li> </ul>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Terminal Services Configuration Guide</i></li> <li>• <i>Cisco IOS Terminal Services Command Reference</i></li> </ul>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Virtual Switch Command Reference</i></li> </ul>	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).  <b>Note</b> For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice Configuration Library</i></li> <li>• <i>Cisco IOS Voice Command Reference</i></li> </ul>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS VPDN Configuration Guide</i></li> <li>• <i>Cisco IOS VPDN Command Reference</i></li> </ul>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.

**Table 1** Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wireless LAN Configuration Guide</i></li> <li>• <i>Cisco IOS Wireless LAN Command Reference</i></li> </ul>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

**Table 2** Cisco IOS Supplementary Documents and Resources

Document Title or Resource	Description
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS releases.
<i>Cisco IOS New, Modified, Removed, and Replaced Commands</i>	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
<i>Cisco IOS Software System Messages</i>	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of <b>debug</b> commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use <a href="#">Cisco MIB Locator</a> .
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: <a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a>

# Additional Resources and Documentation Feedback

*What's New in Cisco Product Documentation* is released monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2008–2009 Cisco Systems, Inc. All rights reserved.



# Using the Command-Line Interface in Cisco IOS Software

---

**Last Updated: October 14, 2009**

This document provides basic information about the command-line interface (CLI) in Cisco IOS software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xi](#)
- [Additional Information, page xii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS Software Documentation](#)” document.

## Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product/Technologies Support area of Cisco.com at <http://www.cisco.com/go/techdocs>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

### Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

---

The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

---

## Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page vii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

## Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

**Table 1** CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the <b>logout</b> or <b>exit</b> command.	<ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display device status.</li> </ul>
Privileged EXEC	From user EXEC mode, issue the <b>enable</b> command.	Router#	Issue the <b>disable</b> command or the <b>exit</b> command to return to user EXEC mode.	<ul style="list-style-type: none"> <li>• Issue <b>show</b> and <b>debug</b> commands.</li> <li>• Copy images to the device.</li> <li>• Reload the device.</li> <li>• Manage device configuration files.</li> <li>• Manage device file systems.</li> </ul>
Global configuration	From privileged EXEC mode, issue the <b>configure terminal</b> command.	Router(config)#	Issue the <b>exit</b> command or the <b>end</b> command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the <b>interface</b> command.	Router(config-if)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the <b>line vty</b> or <b>line console</b> command.	Router(config-line)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the <b>reload</b> command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	rommon # >  The # symbol represents the line number and increments at each prompt.	Issue the <b>continue</b> command.	<ul style="list-style-type: none"> <li>Run as the default operating mode when a valid image cannot be loaded.</li> <li>Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted.</li> <li>Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event.</li> </ul>
Diagnostic (available only on Cisco ASR 1000 series routers)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> <li>A user-configured access policy was configured using the <b>transport-map</b> command, which directed the user into diagnostic mode.</li> <li>The router was accessed using an RP auxiliary port.</li> <li>A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.</li> </ul>	Router(diag)#	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> <li>Inspect various states on the router, including the Cisco IOS state.</li> <li>Replace or roll back the configuration.</li> <li>Provide methods of restarting the Cisco IOS software or other processes.</li> <li>Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components.</li> <li>Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.</li> </ul>

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



**Note**

A keyboard alternative to the **end** command is Ctrl-Z.

## Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes the purpose of the CLI interactive Help commands.

**Table 2** CLI Interactive Help Commands

Command	Purpose
<b>help</b>	Provides a brief description of the Help feature in any command mode.
<b>?</b>	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

### help

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

### ?

```
Router# ?
```

```
Exec commands:
```

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

```
<snip>
```

### partial command?

```
Router(config)# zo?
```

```
zone zone-pair
```

### partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

### command?

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

### command keyword?

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

```
<cr>
```

## Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 3](#) describes these conventions.

**Table 3** CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
WORD domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>

Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

Router(config)# logging host ?
Hostname or A.B.C.D IP address of the syslog server
ipv6 Configure IPv6 syslog server
```

## Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a numeral. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

**Note**

Both password commands have numeric keywords that are single integer values. If you choose a numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable password** or **no enable secret password**.

For more information about password recovery procedures for Cisco products, see [http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_tech\\_note09186a00801746e6.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml).

## Using the Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

**Note**

The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

## Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrp** as a keyword in addition to **version**. (Command and keyword examples are from Cisco IOS Release 12.4(13)T.)

## Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

**Table 4** Default Command Aliases

Command Alias	Original Command
<b>h</b>	help
<b>lo</b>	logout
<b>p</b>	ping
<b>s</b>	show
<b>u</b> or <b>un</b>	undebug
<b>w</b>	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

[http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf\\_a1.html](http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.html).

## Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

## Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebg all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at [http://www.cisco.com/en/US/docs/ios/debug/command/reference/db\\_book.html](http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html).



### Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

## Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

The following three output modifiers are available:

- **begin** *regular-expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular-expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular-expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (`|`), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

## Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

**Table 5** Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following document:

- [Cisco IOS Release 12.4T System Message Guide](#)

## Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved.

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG\_FILE environment variable. The CONFIG\_FILE variable defaults to NVRAM.

## Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*  
[http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf\\_cli-basics.html](http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html)
- Cisco Product/Technology Support  
<http://www.cisco.com/go/techdocs>
- Support area on Cisco.com (also search for documentation by task or product)  
<http://www.cisco.com/en/US/support/index.html>
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)  
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software  
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)  
<http://tools.cisco.com/Support/CLILookup>
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands  
<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2008–2009 Cisco Systems, Inc. All rights reserved.



# Bidirectional Forwarding Detection

---

**First Published: January 14, 2008**

**Last Updated: October 2, 2009**

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Bidirectional Forwarding Detection”](#) section on page 51.

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

- [Prerequisites for Bidirectional Forwarding Detection, page 2](#)
- [Restrictions for Bidirectional Forwarding Detection, page 2](#)
- [Information About Bidirectional Forwarding Detection, page 4](#)
- [How to Configure Bidirectional Forwarding Detection, page 10](#)



---

**Americas Headquarters:**

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

- [Configuration Examples for Bidirectional Forwarding Detection, page 33](#)
- [Additional References, page 48](#)
- [Feature Information for Bidirectional Forwarding Detection, page 51](#)

## Prerequisites for Bidirectional Forwarding Detection

- Cisco Express Forwarding 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 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 Cisco IOS Releases 12.2(33)SRC, 12.2(33)SXH, and 12.2(33)SXI, echo mode is the default.
- The Cisco IOS software incorrectly allows configuration of BFD on virtual-template and dialer interfaces; however, BFD functionality on virtual-template and dialer interfaces is not supported. Avoid configuring BFD on virtual-template and dialer interfaces.
- For Cisco IOS Releases 12.2(18)SXE (and later SX releases), 12.0(31)S, 12.4(4)T, 12.0(32)S, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SRC, and 12.2(33)SB, the Cisco implementation of 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: Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF). In Cisco IOS Release 12.2(33)SRC, BFD supports static routing.
- 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: BGP, EIGRP, IS-IS, and 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.
- 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.
- For Cisco IOS Release 12.2(18)SXH and 12.2(33)SB, the Cisco implementation of BFD supports the following routing protocols: BGP, EIGRP, IS-IS, and OSPF.

- BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away. Multihop configurations are not supported.
- 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.
- For the following Cisco IOS Releases, BFD on PortChannel is not a supported configuration: 12.2SXF, 12.2SRC, and 12.2SRB.
- 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 (ms).
- A maximum of 100 BFD sessions is 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.
- In Cisco IOS Release 12.2(33)SB, BFD is not stateful switchover (SSO) aware, and it is not supported with NSF/SSO and these features should not be used together. Enabling BFD along with NSF/SSO causes the non stop forwarding capability to break during failover since BFD adjacencies are not maintained and the routing clients are forced to mark down adjacencies and reconverge.

#### Cisco IOS Release 12.2(33)SX12 and Cisco Catalyst 6500 Series Switches

- Cisco Catalyst 6500 series switches support up to 100 BFD sessions with a minimum hello interval of 50 ms and a multiplier of 3. The multiplier specifies the minimum number of consecutive packets that can be missed before a session is declared down.
- If SSO is enabled on a dual RP system, the following limitations apply:
  - The maximum number of BFD sessions supported is 50.
  - The minimum hello interval is 500 ms with a multiplier of 3 or higher.
  - If EIGRP is enabled, the maximum number of BFD sessions supported is reduced to 30.
  - Echo mode is supported on Distributed Forwarding Cards (DFCs) only.

- BFD SSO is supported on Cisco Catalyst 6500 series switches using the E-chassis and 67xx line cards only. Centralized Forwarding Cards (CFCs) are not supported.
- To enable echo mode the system must be configured with the **no ip redirects** command.
- During the In Service Software Upgrade (ISSU) cycle the line cards are reset, causing a routing flap in the BFD session.

**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 4](#)
- [Benefits of Using BFD for Failure Detection, page 9](#)

### 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.

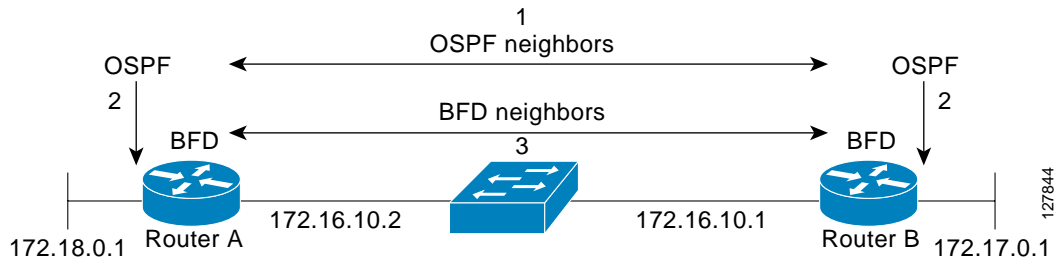
This section includes the following subsections:

- [Neighbor Relationships, page 5](#)
- [BFD Detection of Failures, page 6](#)
- [BFD Version Interoperability, page 6](#)
- [BFD Support on Cisco 12000 Routers, page 6](#)
- [BFD Session Limits, page 7](#)
- [BFD Support for Non Broadcast Media Interfaces, page 7](#)
- [BFD Support for VPN Routing and Forwarding Interfaces, page 7](#)
- [BFD Support for Nonstop Forwarding with Stateful Switchover, page 8](#)
- [BFD Support for Stateful Switchover, page 8](#)
- [BFD Support for Static Routing, page 9](#)

## Neighbor Relationships

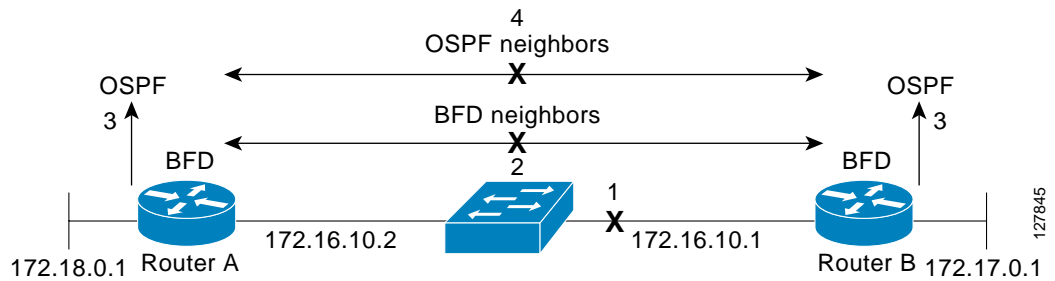
BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols BGP, EIGRP, IS-IS, and OSPF. By sending rapid failure detection notices to the routing protocols in the local router to initiate the routing table recalculation process, BFD contributes to greatly reduced overall network convergence time. [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 negotiations are complete, BFD peers send BFD control packets that act in the same manner as an IGP hello protocol to detect liveness, except at a more accelerated rate. The following information should be noted:

- BFD is a forwarding path failure detection protocol. BFD detects a failure, but the routing protocol must take action to bypass a failed peer.
- Typically, BFD can be used at any protocol layer. However, the Cisco implementation of BFD for Cisco IOS Releases 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. For Cisco IOS Release 12.2(33)SRC, BFD is supported for static routing.
- The Cisco implementation of BFD for Cisco IOS Release 12.2(18)SXE also supports only Layer 3 clients and the EIGRP, IS-IS, and OSPF routing protocols. It does not support the BGP routing protocol.
- 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, if one BFD neighbor is running BFD Version 0 and the other BFD neighbor is running Version 1, the session will run BFD Version 0. The output from the **show bfd neighbors [details]** command will verify which BFD version a BFD neighbor is running.

See the [“Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default: Example”](#) section on page 33 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 the RP and LC as described in the following sections:

- [“BFD Process on the RP”](#) section on page 6
- [“BFD Process on the LC”](#) section on page 7

### 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 the 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 the 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.

### Session 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.

## BFD Session Limits

In Cisco IOS Release 12.2(33)SRC, the number of BFD sessions that can be created has been increased to 128.

## BFD Support for Non Broadcast Media Interfaces

In Cisco IOS Release 12.2(33)SRC, the BFD feature is supported on non broadcast media interfaces including ATM, POS, serial, and VLAN interfaces. BFD support also extends to ATM, frame relay (FR), POS, and serial subinterfaces.

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

## BFD Support for VPN Routing and Forwarding Interfaces

The BFD feature is extended in Cisco IOS Release 12.2(33)SRC to be VPN Routing and Forwarding (VRF) aware to provide fast detection of routing protocol failures between provider edge (PE) and customer edge (CE) routers.

## BFD Support for Nonstop Forwarding with Stateful Switchover

Typically, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Nonstop forwarding (NSF) helps to suppress routing flaps in devices that are enabled with stateful switchover (SSO), thereby reducing network instability.

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

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

In Cisco IOS Release 12.2(33)SRC, BFD sessions are placed in an “Admin Down” state during a planned switchover. The BFD configuration is synched from the active to standby processor, and all BFD clients re-register with the BFD process on the standby processor.

In Cisco IOS Release 12.2(33)SB, BFD is not SSO aware, and it is not supported with NSF/SSO and these features should not be used together. Enabling BFD along with NSF/SSO causes the non stop forwarding capability to break during failover since BFD adjacencies are not maintained and the routing clients are forced to mark down adjacencies and reconverge.

## BFD Support for Stateful Switchover

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

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

### Stateful BFD on the Standby RP

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

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

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

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

## BFD Support for Static Routing

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

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

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

## Benefits of Using BFD for Failure Detection

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

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

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

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

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

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

# How to Configure Bidirectional Forwarding Detection

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 Release 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 place 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 10](#) (required)
- [Configuring BFD Support for Dynamic Routing Protocols, page 11](#) (required)
- [Configuring BFD Support for Static Routing, page 25](#) (optional)
- [Configuring BFD Echo Mode, page 27](#) (optional)
- [Monitoring and Troubleshooting BFD, page 29](#) (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	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type number</code>  <b>Example:</b> Router(config)# interface FastEthernet 6/0	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	<pre>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</pre> <p><b>Example:</b> Router(config-if)# bfd interval 50 min_rx 50 multiplier 5</p>	Enables BFD on the interface.
Step 5	<pre>end</pre> <p><b>Example:</b> Router(config-if)# end</p>	Exits interface configuration mode and returns to privileged EXEC mode.

## Configuring BFD Support for Dynamic Routing Protocols

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

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

For Cisco IOS Release 12.2(33)SRC, you may configure BFD support for static routing.

For Cisco IOS Releases 12.0(31)S and 12.4(4)T, you may 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 may 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 11](#) (optional)
- [Configuring BFD Support for EIGRP, page 13](#) (optional)
- [Configuring BFD Support for IS-IS, page 15](#) (optional)
- [Configuring BFD Support for OSPF, page 19](#) (optional)
- [Configuring BFD Support for HSRP, page 23](#) (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 10](#) 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp <i>as-tag</i></b>  <b>Example:</b> Router(config)# router bgp tag1	Specifies a BGP process and enters router configuration mode.
Step 4	<b>neighbor <i>ip-address</i> fall-over bfd</b>  <b>Example:</b> Router(config-router)# neighbor 172.16.10.2 fall-over bfd	Enables BFD support for fallover.
Step 5	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and returns the router to privileged EXEC mode.

	Command or Action	Purpose
Step 6	<pre>show bfd neighbors [details]</pre> <p><b>Example:</b> Router# show bfd neighbors detail</p>	<p>(Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered.</p> <p><b>Note</b> In order to display the full output of the <b>show bfd neighbors details</b> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <b>attach slot-number</b> command to establish a CLI session with a line card. The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> command when it is entered on a line card.</p>
Step 7	<pre>show ip bgp neighbor</pre> <p><b>Example:</b> Router# show ip bgp neighbor</p>	<p>(Optional) Displays information about BGP and TCP connections to neighbors.</p>

## What to Do Next

See the “[Monitoring and Troubleshooting BFD](#)” section on page 29 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 13](#)
- [Configuring BFD Support for IS-IS, page 15](#)
- [Configuring BFD Support for OSPF, page 19](#)
- [Configuring BFD Support for HSRP, page 23](#)

## 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 10 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. **bfd all-interfaces**  
or  
**bfd interface** *type number*
5. **end**
6. **show bfd neighbors** [**details**]
7. **show ip eigrp interfaces** [*type number*] [*as-number*] [**detail**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router eigrp 123	Configures the EIGRP routing process and enters router configuration mode.
Step 4	<b>bfd all-interfaces</b>  or  <b>bfd interface</b> <i>type number</i>  <b>Example:</b> Router(config-router)# bfd all-interfaces  or  <b>Example:</b> 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 5	<b>end</b>  <b>Example:</b> Router(config-router) end	Exits router configuration mode and returns the router to privileged EXEC mode.

Command or Action	Purpose
<p><b>Step 6</b> <code>show bfd neighbors [details]</code></p> <p><b>Example:</b> Router# show bfd neighbors details</p>	<p>(Optional) Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered.</p> <p><b>Note</b> In order to see the full output of the <b>show bfd neighbors details</b> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <b>attach slot-number</b> command to establish a CLI session with a line card. The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> command when it is entered on a line card.</p>
<p><b>Step 7</b> <code>show ip eigrp interfaces [type number] [as-number] [detail]</code></p> <p><b>Example:</b> Router# show ip eigrp interfaces detail</p>	<p>(Optional) Displays the interfaces for which BFD support for EIGRP has been enabled.</p>

## What to Do Next

See the “[Monitoring and Troubleshooting BFD](#)” section on page 29 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 11](#)
- [Configuring BFD Support for IS-IS, page 15](#)
- [Configuring BFD Support for OSPF, page 19](#)
- [Configuring BFD Support for HSRP, page 23](#)

## Configuring BFD Support for IS-IS

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

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

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

- [Configuring BFD Support for IS-IS for All Interfaces, page 16](#)
- [Configuring BFD Support for IS-IS for One or More Interfaces, page 18](#)

## 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 10](#) for more information.

## Configuring BFD Support for IS-IS for All Interfaces

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>router isis area-tag</code>  <b>Example:</b> <code>Router(config)# router isis tag1</code>	Specifies an IS-IS process and enters router configuration mode.
Step 4	<code>bfd all-interfaces</code>  <b>Example:</b> <code>Router(config-router)# bfd all-interfaces</code>	Enables BFD globally on all interfaces associated with the IS-IS routing process.

	Command or Action	Purpose
Step 5	<code>exit</code>  <b>Example:</b> Router(config-router)# exit	(Optional) Returns the router to global configuration mode.
Step 6	<code>interface type number</code>  <b>Example:</b> Router(config)# interface fastethernet 6/0	(Optional) Enters interface configuration mode.
Step 7	<code>ip router isis [tag]</code>  <b>Example:</b> Router(config-if)# ip router isis tag1	(Optional) Enables support for IPv4 routing on the interface.
Step 8	<code>isis bfd [disable]</code>  <b>Example:</b> Router(config-if)# isis bfd	(Optional) Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process.  <b>Note</b> You should use the <b>disable</b> keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the <b>bfd all-interfaces</b> command in router configuration mode.
Step 9	<code>end</code>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 10	<code>show bfd neighbors [details]</code>  <b>Example:</b> Router# show bfd neighbors details	(Optional) Displays information that can be used to verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.  <b>Note</b> In order to display the full output of the <b>show bfd neighbors details</b> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <b>attach slot-number</b> command to establish a CLI session with a line card. The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> command when it is entered on a line card.
Step 11	<code>show clns interface</code>  <b>Example:</b> Router# show clns interface	(Optional) Displays information that can be used to verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

## What to Do Next

See the [“Monitoring and Troubleshooting BFD”](#) section on page 29 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 18.

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

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type number</code>  <b>Example:</b> Router(config)# interface fastethernet 6/0	Enters interface configuration mode.
Step 4	<code>ip router isis [tag]</code>  <b>Example:</b> Router(config-if)# ip router isis tag1	Enables support for IPv4 routing on the interface.
Step 5	<code>isis bfd [disable]</code>  <b>Example:</b> 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.  <b>Note</b> You should use the <b>disable</b> keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the <b>bfd all-interfaces</b> command in router configuration mode.
Step 6	<code>end</code>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns the router to privileged EXEC mode.

Command or Action	Purpose
<p><b>Step 7</b> <code>show bfd neighbors [details]</code></p> <p><b>Example:</b> Router# show bfd neighbors details</p>	<p>(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.</p> <p><b>Note</b> In order to display the full output of the <b>show bfd neighbors details</b> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <b>attach slot-number</b> command to establish a CLI session with a line card. The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> command when it is entered on a line card.</p>
<p><b>Step 8</b> <code>show clns interface</code></p> <p><b>Example:</b> Router# show clns interface</p>	<p>(Optional) Displays information that can help verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.</p>

## What to Do Next

See the “[Monitoring and Troubleshooting BFD](#)” section on page 29 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 11](#)
- [Configuring BFD Support for EIGRP, page 13](#)
- [Configuring BFD Support for OSPF, page 19](#)
- [Configuring BFD Support for HSRP, page 23](#)

## 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 20](#) (optional)
- [Configuring BFD Support for OSPF for One or More Interfaces, page 22](#) (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 22.

### 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 10 for more information.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>router ospf process-id</code>  <b>Example:</b> <code>Router(config)# router ospf 4</code>	Specifies an OSPF process and enters router configuration mode.

	Command or Action	Purpose
Step 4	<code>bfd all-interfaces</code>  <b>Example:</b> Router(config-router)# <code>bfd all-interfaces</code>	Enables BFD globally on all interfaces associated with the OSPF routing process.
Step 5	<code>exit</code>  <b>Example:</b> Router(config-router)# <code>exit</code>	(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	<code>interface type number</code>  <b>Example:</b> Router(config)# <code>interface fastethernet 6/0</code>	(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	<code>ip ospf bfd [disable]</code>  <b>Example:</b> Router(config-if)# <code>ip ospf bfd disable</code>	(Optional) Disables BFD on a per-interface basis for one or more interfaces associated with the OSPF routing process.  <b>Note</b> You should use the <b>disable</b> keyword only if you enabled BFD on all of the interfaces that OSPF is associated with using the <b>bfd all-interfaces</b> command in router configuration mode.
Step 8	<code>end</code>  <b>Example:</b> Router(config-if)# <code>end</code>	Exits interface configuration mode and returns the router to privileged EXEC mode.
Step 9	<code>show bfd neighbors [details]</code>  <b>Example:</b> Router# <code>show bfd neighbors detail</code>	(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.  <b>Note</b> In order to display the full output of the <b>show bfd neighbors details</b> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <b>attach slot-number</b> command to establish a CLI session with a line card. The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> command when it is entered on a line card.
Step 10	<code>show ip ospf</code>  <b>Example:</b> Router# <code>show ip ospf</code>	(Optional) Displays information that can help verify if BFD for OSPF has been enabled.

## What to Do Next

See the “[Monitoring and Troubleshooting BFD](#)” section on page 29 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 11
- [Configuring BFD Support for EIGRP](#), page 13
- [Configuring BFD Support for IS-IS](#), page 15
- [Configuring BFD Support for HSRP](#), page 23

## 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 10 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	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type number</code>  <b>Example:</b> Router(config)# interface fastethernet 6/0	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	<pre>ip ospf bfd [disable]</pre> <p><b>Example:</b> Router(config-if)# ip ospf bfd</p>	<p>Enables or disables BFD on a per-interface basis for one or more interfaces associated with the OSPF routing process.</p> <p><b>Note</b> You should use the <b>disable</b> keyword only if you enabled BFD on all of the interfaces that OSPF is associated with using the <b>bfd all-interfaces</b> command in router configuration mode.</p>
Step 5	<pre>end</pre> <p><b>Example:</b> Router(config-if)# end</p>	<p>Exits interface configuration mode and returns the router to privileged EXEC mode.</p>
Step 6	<pre>show bfd neighbors [details]</pre> <p><b>Example:</b> Router# show bfd neighbors details</p>	<p>(Optional) Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered.</p> <p><b>Note</b> In order to display the full output of the <b>show bfd neighbors details</b> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <b>attach slot-number</b> command to establish a CLI session with a line card. The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> command when it is entered on a line card.</p>
Step 7	<pre>show ip ospf</pre> <p><b>Example:</b> Router# show ip ospf</p>	<p>(Optional) Displays information that can help verify if BFD support for OSPF has been enabled.</p>

## What to Do Next

See the “[Monitoring and Troubleshooting BFD](#)” section on page 29 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 11
- [Configuring BFD Support for EIGRP](#), page 13
- [Configuring BFD Support for IS-IS](#), page 15
- [Configuring BFD Support for HSRP](#), page 23

## 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 reenble 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 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef	Enables Cisco Express Forwarding or distributed Cisco Express Forwarding.
Step 4	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface FastEthernet 6/0	Enters interface configuration mode.
Step 5	<b>ip address</b> <i>ip-address mask</i>  <b>Example:</b> Router(config-if)# ip address 10.0.0.11 255.255.255.0	Configures an IP address for the interface.

	Command or Action	Purpose
Step 6	<pre>standby [group-number] ip [ip-address] [secondary]]</pre> <p><b>Example:</b> Router(config-if)# standby 1 ip 10.0.0.11 </p>	Activates HSRP.
Step 7	<pre>standby bfd</pre> <p><b>Example:</b> Router(config-if)# standby bfd </p>	(Optional) Enables HSRP support for BFD on the interface.
Step 8	<pre>exit</pre> <p><b>Example:</b> Router(config-if)# exit </p>	Exits interface configuration mode.
Step 9	<pre>standby bfd all-interfaces</pre> <p><b>Example:</b> Router(config)# standby bfd all-interfaces </p>	(Optional) Enables HSRP support for BFD on all interfaces.
Step 10	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit </p>	Exits global configuration mode.
Step 11	<pre>show standby neighbors</pre> <p><b>Example:</b> Router# show standby neighbors </p>	(Optional) Displays information about HSRP support for BFD.

## What to Do Next

See the “[Monitoring and Troubleshooting BFD](#)” section on page 29 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 11
- [Configuring BFD Support for EIGRP](#), page 13
- [Configuring BFD Support for IS-IS](#), page 15
- [Configuring BFD Support for OSPF](#), page 19

## Configuring BFD Support for Static Routing

Perform this task to configure BFD support for static routing.

Repeat the steps in this procedure on each BFD neighbor. For more information, see the “[Configuring BFD Support for Static Routing: Example](#)” section on page 47.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **bfd interval** *milliseconds min\_rx milliseconds multiplier interval-multiplier*
6. **ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*
7. **ip route** *prefix mask {ip-address | interface-type interface-number [ip-address]}* [**dhcp**] [*distance*] [*name next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
8. **end**
9. **show ip static route**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface serial 2/0	Configures an interface and enters interface configuration mode.
Step 4	<b>ip address</b> <i>ip-address mask</i>  <b>Example:</b> Router(config-if)# ip address 10.201.201.1 255.255.255.0	Configures an IP address for the interface.
Step 5	<b>bfd interval</b> <i>milliseconds min_rx milliseconds multiplier interval-multiplier</i>  <b>Example:</b> Router(config-if)# bfd interval 500 min_rx 500 multiplier 5	Enables BFD on the interface.
Step 6	<b>ip route static bfd</b> [ <b>vrf</b> <i>vrf-name</i> ] <i>interface-type interface-number gateway</i>  <b>Example:</b> Router(config-if)# ip route static bfd Serial 2/0 10.201.201.2	Specifies a static route BFD neighbor. <ul style="list-style-type: none"> <li>• The <i>interface-type interface-number</i> and <i>gateway</i> arguments are required because BFD support exists only for directly connected neighbors.</li> </ul>

	Command or Action	Purpose
Step 7	<pre>ip route prefix mask {ip-address   interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent   track number] [tag tag]</pre> <p><b>Example:</b> Router(config-if)# ip route 10.0.0.0 255.0.0.0 Serial 2/0 10.201.201.2</p>	Specifies a static route BFD neighbor.
Step 8	<pre>end</pre> <p><b>Example:</b> Router(config-if)# end</p>	Exits interface configuration mode and returns to privileged EXEC mode.
Step 9	<pre>show ip static route</pre> <p><b>Example:</b> Router# show ip static route</p>	(Optional) Displays the static process local Routing Information Base (RIB) information.

## 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 27](#)
- [Prerequisites, page 27](#)
- [Restrictions, page 28](#)

## 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 10](#) 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 28](#)
- [Disabling BFD Echo Mode Without Asymmetry, page 29](#)

## 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	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>bfd slow-timer milliseconds</code>  <b>Example:</b> <code>Router(config)# bfd slow-timer 12000</code>	Configures the BFD slow timer.
Step 4	<code>end</code>  <b>Example:</b> <code>Router(config)# end</code>	Exits global configuration mode and returns the router to privileged EXEC mode.

## Disabling BFD Echo Mode Without Asymmetry

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

Repeat the steps in this procedure for each BFD router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bfd echo**
4. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>bfd echo</pre> <p><b>Example:</b> Router(config)# no bfd echo</p>	Enables BFD echo mode. <ul style="list-style-type: none"> <li>• Use the <b>no</b> form to disable BFD echo mode.</li> </ul>
Step 4	<pre>end</pre> <p><b>Example:</b> Router(config)# end</p>	Exits global configuration mode and returns the router to privileged EXEC 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 4](#).

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

- [Monitoring and Troubleshooting BFD for Cisco 7600 Series Routers, page 30](#)
- [Monitoring and Troubleshooting BFD for Cisco 12000 Series Routers, page 30](#)
- [Monitoring and Troubleshooting BFD for Cisco 10720 Internet Routers, page 32](#)

## 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	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>show bfd neighbors [details]</pre> <p><b>Example:</b> Router# show bfd neighbors details </p>	(Optional) Displays the BFD adjacency database. <ul style="list-style-type: none"> <li>• The <b>details</b> keyword shows all BFD protocol parameters and timers per neighbor.</li> </ul> <p><b>Note</b> In order to see the full output of the <b>show bfd neighbors details</b> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <b>attach slot-number</b> command to establish a CLI session with a line card. The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> command when it is entered on a line card.</p>
Step 3	<pre>debug bfd [packet   event]</pre> <p><b>Example:</b> Router# debug bfd packet </p>	(Optional) 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	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>attach slot-number</pre> <p><b>Example:</b> Router# attach 6 </p>	<p>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.</p> <ul style="list-style-type: none"> <li>If the slot number is omitted, you are prompted for the slot number.</li> </ul> <p><b>Note</b> In order to display the full output of the <code>show bfd neighbors details</code> command on a Cisco 12000 series router, you must enter the command on the line card. Enter the <code>attach slot-number</code> command to establish a CLI session with a line card.</p>
Step 3	<pre>show bfd neighbors [details]</pre> <p><b>Example:</b> Router# show bfd neighbors details </p>	<p>Displays the BFD adjacency database.</p> <ul style="list-style-type: none"> <li>The <code>details</code> keyword shows all BFD protocol parameters and timers per neighbor.</li> </ul> <p><b>Note</b> The registered protocols are not shown in the output of the <code>show bfd neighbors details</code> when it is entered on a line card.</p>
Step 4	<pre>show monitor event-trace bfd [all]</pre> <p><b>Example:</b> Router# show monitor event-trace bfd all </p>	<p>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.</p>
Step 5	<pre>debug bfd event</pre> <p><b>Example:</b> Router# debug bfd event </p>	<p>Displays debugging information about BFD state transitions.</p>
Step 6	<pre>debug bfd packet</pre> <p><b>Example:</b> Router# debug bfd packet </p>	<p>Displays debugging information about BFD control packets.</p>

	Command or Action	Purpose
Step 7	<pre>debug bfd ipc-error</pre> <p><b>Example:</b> Router# debug bfd ipc-error</p>	Displays debugging information with IPC errors on the RP and LC.
Step 8	<pre>debug bfd ipc-event</pre> <p><b>Example:</b> Router# debug bfd ipc-event</p>	Displays debugging information with IPC events on the RP and LC.
Step 9	<pre>debug bfd oir-error</pre> <p><b>Example:</b> Router# debug bfd oir-error</p>	Displays debugging information with OIR errors on the RP and LC.
Step 10	<pre>debug bfd oir-event</pre> <p><b>Example:</b> Router# debug bfd oir-event</p>	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	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>show bfd neighbors [details]</pre> <p><b>Example:</b> Router# show bfd neighbors details</p>	(Optional) Displays the BFD adjacency database. <ul style="list-style-type: none"> <li>• The <b>details</b> keyword will show all BFD protocol parameters and timers per neighbor.</li> </ul> <p><b>Note</b> The registered protocols are not shown in the output of the <b>show bfd neighbors details</b> when it is entered on a line card.</p>

	Command or Action	Purpose
Step 3	<code>debug bfd event</code>	(Optional) Displays debugging information about BFD state transitions.
	<b>Example:</b> <code>Router# debug bfd event</code>	
Step 4	<code>debug bfd packet</code>	(Optional) Displays debugging information about BFD control packets.
	<b>Example:</b> <code>Router# debug bfd packet</code>	

## 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, page 33](#)
- [Configuring BFD in an OSPF Network: Example, page 38](#)
- [Configuring BFD in a BGP Network: Example, page 42](#)
- [Configuring BFD in an IS-IS Network: Example, page 45](#)
- [Configuring BFD in an HSRP Network: Example, page 46](#)
- [Configuring BFD Support for Static Routing: Example, page 47](#)

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

#### Cisco IOS Release 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 RouterA 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 control packets for BFD sessions and failure detections.

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

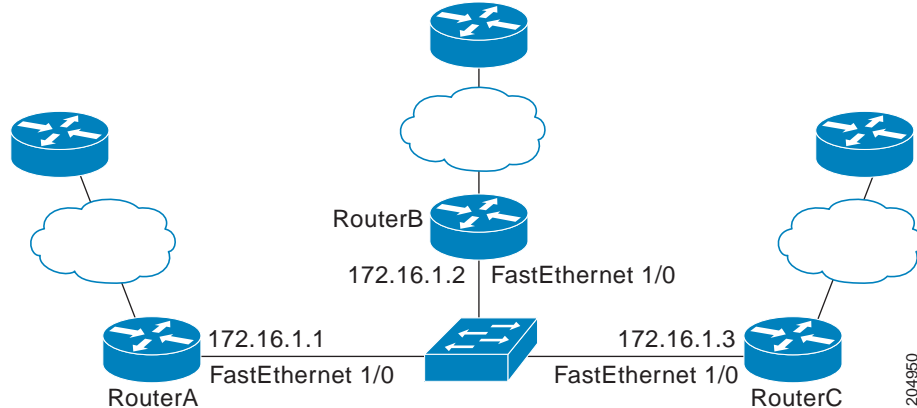


Figure 3 shows a large EIGRP network with several routers, three of which are BFD neighbors that are running EIGRP as their routing protocol.

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

```
end
```

### Configuration for RouterB

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

### Configuration for RouterC

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

```

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

RouterA

RouterA# **show bfd neighbors details**

```

OurAddr      NeighAddr      LD/RD RH/RS   Holddown(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   Holddown(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
Holddown (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  Holddown(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
Holddown (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  Holddown(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
Holddown (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

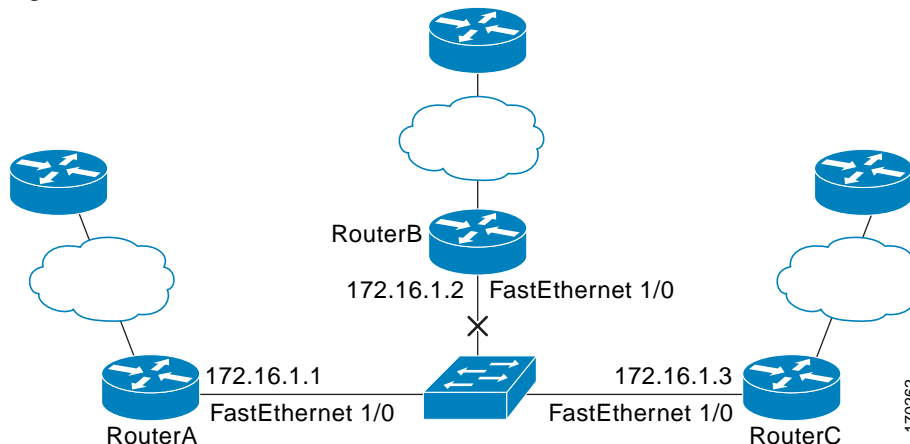


Figure 4 shows that Fast Ethernet interface 0/1 on RouterB has failed. Without this neighbor, there is no way to reach the network beyond RouterB.

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
<b>172.16.1.1</b>	<b>172.16.1.3</b>	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
<b>172.16.1.3</b>	<b>172.16.1.1</b>	3/5	1	114 (3)	Up	Fa0/1

## Configuring BFD in an OSPF Network: Example

### Cisco IOS Release 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 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
BFD is enabled
  Area BACKBONE(0)
    Number of interfaces in this area is 2 (1 loopback)
```

```

Area has no authentication
SPF algorithm last executed 00:00:08.828 ago
SPF algorithm executed 9 times
Area ranges are
Number of LSA 3. Checksum Sum 0x028417
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```

## 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 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
BFD is enabled
  Area BACKBONE(0)
    Number of interfaces in this area is 2 (1 loopback)
    Area has no authentication
    SPF algorithm last executed 02:07:30.932 ago
    SPF algorithm executed 7 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x28417
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

```

The output 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

### Cisco IOS Release 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  Holddown(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
Holddown (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

### Cisco IOS Release 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 !
```

## Configuring BFD Support for Static Routing: Example

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

**Router A**

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

**Router B**

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

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

## Additional References

The following sections provide references related to the BFD feature.

## Related Documents

Related Topic	Document Title
Configuring and monitoring BGP	<a href="#">“Cisco BGP Overview”</a> module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
Configuring and monitoring EIGRP	<a href="#">“Configuring EIGRP”</a> module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
Configuring and monitoring HSRP	<a href="#">“Configuring HSRP”</a> module of the <i>Cisco IOS IP Application Services Configuration Guide</i>
Configuring and monitoring IS-IS	<a href="#">“Configuring Integrated IS-IS”</a> module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
Configuring and monitoring OSPF	<a href="#">“Configuring OSPF”</a> module of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
BFD commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Routing: Protocol-Independent Command Reference</a>
BGP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Routing: Protocol-Independent Command Reference</a>
EIGRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Routing: Protocol-Independent Command Reference</a>

Related Topic	Document Title
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Application Services Command Reference</a>
IS-IS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Routing: Protocol-Independent Command Reference</a>
OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Routing: Protocol-Independent Command Reference</a>

## Standards

Standard	Title
IETF Draft	<i>Bidirectional Forwarding Detection</i> , February 2009 ( <a href="http://www.ietf.org/internet-drafts/draft-ietf-bfd-base-09.txt">http://www.ietf.org/internet-drafts/draft-ietf-bfd-base-09.txt</a> )
IETF Draft	<i>BFD for IPv4 and IPv6 (Single Hop)</i> , February 2009 ( <a href="http://www.ietf.org/internet-drafts/draft-ietf-bfd-v4v6-1hop-09.txt">http://www.ietf.org/internet-drafts/draft-ietf-bfd-v4v6-1hop-09.txt</a> )

## 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:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

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

# Feature Information for Bidirectional Forwarding Detection

Table 1 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



**Note**

Table 1 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 1** Feature Information for Bidirectional Forwarding Detection

Feature Name	Releases	Feature Information
Bidirectional Forwarding Detection (standard implementation, Version 1)	12.2(18)SXE 12.0(31)S 12.0(32)S 12.4(9)T 12.2(33)SRB 12.4(11)T 12.4(15)T 12.2(33)SXH 12.2(33)SRC	<p>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.</p> <p>In Release 12.0(31)S, support was added for the Cisco 12000 series Internet router.</p> <p>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.</p>

Table 1 Feature Information for Bidirectional Forwarding Detection (continued)

Feature Name	Releases	Feature Information
BFD Echo Mode	12.4(9)T 12.2(33)SRB	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring BFD Echo Mode, page 27</a></li> <li>• <a href="#">Disabling BFD Echo Mode Without Asymmetry, page 29</a></li> </ul>
BFD—EIGRP Support	12.0(31)S 12.4(4)T 12.2(18)SXE 12.2(33)SRA 12.2(33)SRB	<p>BFD support for EIGRP can be configured so that EIGRP is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD.</p> <p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring BFD Support for Dynamic Routing Protocols, page 11</a></li> <li>• <a href="#">Configuring BFD Support for EIGRP, page 13</a></li> <li>• <a href="#">Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default: Example, page 33</a></li> </ul>
BFD—VRF Support	12.2(33)SRC 15.0(1)M	<p>The BFD feature support is extended to be VPN Routing and Forwarding (VRF) aware to provide fast detection of routing protocol failures between provider edge (PE) and customer edge (CE) routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BFD Support for VPN Routing and Forwarding Interfaces, page 7</a></li> </ul>

**Table 1** Feature Information for Bidirectional Forwarding Detection (continued)

Feature Name	Releases	Feature Information
BFD—WAN Interface Support	12.2(33)SRC 15.0(1)M	<p>BFD feature is supported on non broadcast media interfaces including ATM, POS, serial, and VLAN interfaces. BFD support also extends to ATM, FR, POS, and serial subinterfaces.</p> <p>The <b>bfd interval</b> command must be configured on the interface to initiate BFD monitoring.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BFD Support for Non Broadcast Media Interfaces, page 7</a></li> </ul>
HSRP Support for BFD	12.4(11)T 12.4(15)T 12.2(33)SRC	<p>In Release 12.4(11)T, support for HSRP was added.</p> <p>In Release 12.4(15)T, BFD is supported on the Integrated Services Router (ISR) family of Cisco routers, for example, the Cisco 3800 ISR series routers.</p> <p>In Release 12.2(33)SRC, the number of BFD sessions that can be created has been increased, BFD support has been extended to ATM, FR, POS, and serial subinterfaces, the BFD feature has been extended to be VRF-aware, BFD sessions are placed in an “Admin Down” state during a planned switchover, and BFD support has been extended to static routing.</p> <p>The following section provides information about this feature:</p> <p><a href="#">Configuring BFD in an HSRP Network: Example, page 46</a></p>
IS-IS Support for BFD over IPv4	12.0(31)S 12.4(4)T 12.2(18)SXE 12.2(33)SRA	<p>BFD support for OSPF can be configured globally on all interfaces or configured selectively on one or more interfaces. When BFD support is configured with IS-IS as a registered protocol with BFD, IS-IS receives forwarding path detection failure messages from BFD.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring BFD Support for Dynamic Routing Protocols, page 11</a></li> <li>• <a href="#">Configuring BFD Support for IS-IS, page 15</a></li> <li>• <a href="#">Configuring BFD in an IS-IS Network: Example, page 45</a></li> </ul>

Table 1 Feature Information for Bidirectional Forwarding Detection (continued)

Feature Name	Releases	Feature Information
OSPF Support for BFD over IPv4	12.0(31)S 12.4(4)T 12.2(18)SXE 12.2(33)SRA	<p>BFD support for OSPF can be configured globally on all interfaces or configured selectively on one or more interfaces. When BFD support is configured with OSPF as a registered protocol with BFD, OSPF receives forwarding path detection failure messages from BFD.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring BFD Support for Dynamic Routing Protocols, page 11</a></li> <li>• <a href="#">Configuring BFD Support for OSPF, page 19</a></li> <li>• <a href="#">Configuring BFD in an OSPF Network: Example, page 38</a></li> </ul>
SSO—BFD	12.2(33)SXI2	<p>Network deployments that use dual RP routers and switches have a graceful restart mechanism to protect forwarding states across a switchover. This feature enables BFD to maintain sessions in a up state across switchovers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BFD Support for Stateful Switchover, page 8</a></li> </ul>
SSO—BFD (Admin Down)	12.2(33)SRC	<p>To support SSO, BFD sessions are placed in an “Admin Down” state during a planned switchover. The BFD configuration is synched from the active to standby processor, and all BFD clients re-register with the BFD process on the standby processor.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BFD Support for Nonstop Forwarding with Stateful Switchover, page 8</a></li> </ul>
Static Routes for BFD	12.2(33)SRC 15.0(1)M	<p>Unlike dynamic routing protocols, such as OSPF and BGP, static routing has no method of peer discovery. Therefore, when BFD is configured, the reachability of the gateway is completely dependent on the state of the BFD session to the specified neighbor. Unless the BFD session is up, the gateway for the static route is considered unreachable, and therefore the affected routes will not be installed in the appropriate RIB.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BFD Support for Static Routing, page 9</a></li> <li>• <a href="#">Configuring BFD Support for Static Routing, page 25</a></li> <li>• <a href="#">Configuring BFD Support for Static Routing: Example, page 47</a></li> </ul>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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.

© 2008–2009 Cisco Systems, Inc. All rights reserved.

