



## MPLS Traffic Engineering Fast Reroute— Link Protection

---

This feature module describes the Fast Reroute (FRR) link protection feature of Multiprotocol Label Switching (MPLS) traffic engineering (TE).

Regular MPLS traffic engineering automatically establishes and maintains label-switched paths (LSPs) across the backbone using Resource Reservation Protocol (RSVP). The path used by a given LSP is based on the LSP resource requirements and available network resources such as bandwidth.

Available resources are flooded via extensions to a link-state based Interior Gateway Protocol (IGP), such as Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).

Paths for LSPs are calculated at the LSP headend. Under failure conditions, the headend determines a new route for the LSP. Recovery at the headend provides for the optimal use of resources. However, due to messaging delays, the headend cannot recover as fast as possible by making a repair at the point of failure.

Fast Reroute provides link protection to LSPs. This enables all traffic carried by LSPs that traverse a failed link to be rerouted around the failure. The reroute decision is completely controlled locally by the router interfacing the failed link. The headend of the tunnel is also notified of the link failure through the IGP or through RSVP; the headend then attempts to establish a new LSP that bypasses the failure.



### Note

---

Local reroute prevents any further packet loss caused by the failed link. This gives the headend of the tunnel time to reestablish the tunnel along a new, optimal route. If the headend still cannot find another path to take, it continues using the backup tunnel.

---

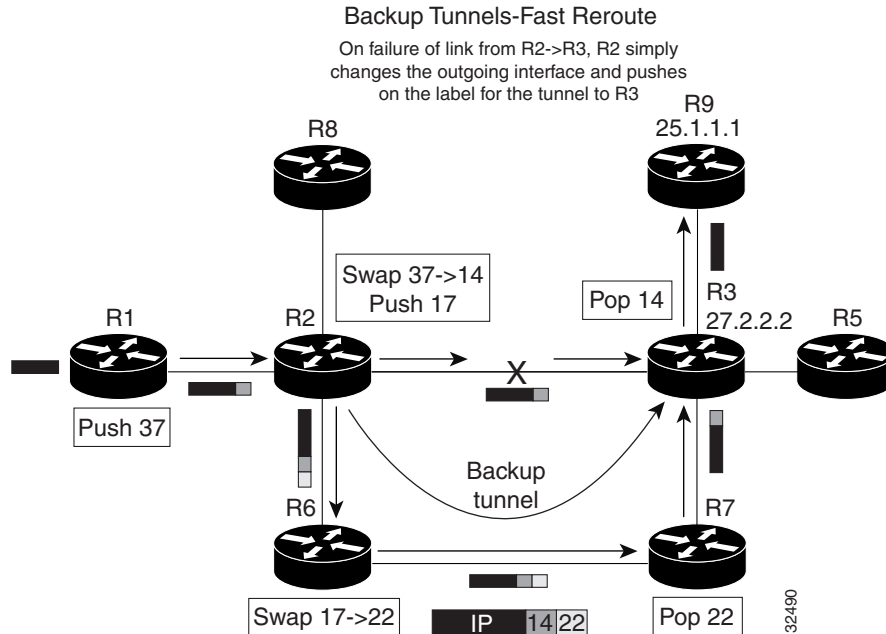
### Fast Reroute Operation

The example in [Figure 1](#) illustrates how Fast Reroute link protection is used to protect traffic carried in a TE tunnel between devices R1 and R9, as it traverses the midpoint link between devices R2 and R3. The TE tunnel from R1 to R9 is considered to be the primary tunnel and is defined by labels 37, 14, and Pop. To protect that R2–R3 link, you create a backup tunnel that runs from R2 to R3 by way of R6 and R7. This backup tunnel is defined by labels 17, 22, and Pop.

When R2 is notified that the link between it and R3 is no longer available, it simply forwards traffic destined for R3 through the backup tunnel. That is accomplished by pushing label 17 onto packets destined to R3 after the normal swap operation (which replaces label 37 with label 14) has been

performed. Pushing label 17 onto packets forwards them along the backup tunnel, thereby routing traffic around the failed link. The decision to reroute packets from the primary tunnel to the backup tunnel is made solely by R2 upon detection of link failure.

**Figure 1 Backup Tunnel—Fast Reroute**



The Fast Reroute feature has two noticeable benefits: the increased reliability it gives to IP traffic service and the high scalability inherent in its design:

- **Increased Reliability for IP Services**—MPLS traffic engineering with Fast Reroute uses failover times that match the capabilities of SONET link restoration. This leverages a very high degree of resiliency for IP traffic that flows over a service provider's backbone, leading to more robust IP services and higher end-customer satisfaction.
- **High Scalability Solution**—The Fast Reroute feature uses the highest degree of scalability by supporting the mapping of all primary tunnels that traverse a link onto a single backup tunnel. This capability bounds the growth of backup tunnels to the number of links in the backbone rather than the number of TE tunnels that run across the backbone.

#### Feature History for MPLS Traffic Engineering Fast Reroute Link Protection

Release	Modification
12.0(10) ST	This feature was introduced.
12.0(16) ST	Support was added for Cisco Series 7200 and 7500 platforms.
12.0(26)S	Support was added for Cisco Series 10000 platform.

#### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

# Contents

- [Prerequisites for MPLS Traffic Engineering Fast Reroute Link Protection, page 3](#)
- [Restrictions for MPLS Traffic Engineering Fast Reroute Link Protection, page 3](#)
- [How to Configure Fast Reroute Link Protection, page 3](#)
- [Verifying that MPLS Traffic Engineering Fast Reroute Link Protection Has Been Enabled, page 9](#)
- [Configuration Examples for MPLS Traffic Engineering Fast Reroute Link Protection, page 9](#)
- [Additional References, page 10](#)
- [Glossary, page 12](#)

## Prerequisites for MPLS Traffic Engineering Fast Reroute Link Protection

Your network must support both of the following Cisco IOS features before you can enable Fast Reroute link protection:

- IP Cisco Express Forwarding (CEF)
- Multiprotocol Label Switching

At the same time, the network must support at least one of the following protocols:

- IS-IS
- OSPF

## Restrictions for MPLS Traffic Engineering Fast Reroute Link Protection

The Fast Reroute link protection feature works only on the following:

- Packet over SONET (POS) links (SDH in the European standard)
- Links that use MPLS global label allocation (GLA)

## How to Configure Fast Reroute Link Protection

This section contains the following procedures:

- [Configuring a Tunnel for Fast Reroute Link Protection, page 4](#) (required)
- [Establishing a Backup Tunnel Around the Link to be Protected, page 6](#) (required)
- [Configuring the Protected Link to Use the Backup Tunnel, page 7](#) (required)

Before or after entering the commands described in these procedures, you must enable the MPLS traffic engineering tunnel capability globally on the tunnel routers by entering the **mpls traffic-eng tunnels** command.

## Configuring a Tunnel for Fast Reroute Link Protection

Perform this task to configure the head-end of a primary tunnel (router R1 in [Figure 1](#)) and assign it for Fast Reroute protection.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip unnumbered** *type number*
5. **tunnel destination** *A.B.C.D*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng autoroute announce**
8. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
9. **tunnel mpls traffic-eng bandwidth** [*sub-pool* | *global*] *bandwidth*
10. **tunnel mpls traffic-eng path-option** *number* { *dynamic* | **explicit** { *name path-name* | *path-number* } } [*lockdown*]
11. **tunnel mpls traffic-eng fast-reroute**

### 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> [ <i>name-tag</i> ]  <b>Example:</b> Router(config)# interface Tunnel1	Creates a tunnel interface and enters interface configuration mode.
Step 4	<b>ip unnumbered</b> <i>type number</i>  <b>Example:</b> Router(config-if)# ip unnumbered loopback0	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 5	<b>tunnel destination</b> <i>A.B.C.D</i>  <b>Example:</b> Router(config-if)# tunnel destination 27.2.2.2	Specifies the destination of a tunnel interface.

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 6</b>	<pre>tunnel mode mpls traffic-eng</pre> <p><b>Example:</b> Router(config-if)# tunnel mode mpls traffic-eng</p>	Sets the mode of a tunnel to MPLS for traffic engineering.
<b>Step 7</b>	<pre>tunnel mpls traffic-eng autoroute announce</pre> <p><b>Example:</b> Router(config-if)# tunnel mpls traffic-eng autoroute announce</p>	Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced SPF calculation.
<b>Step 8</b>	<pre>tunnel mpls traffic-eng priority setup-priority [hold-priority]</pre> <p><b>Example:</b> Router(config-if)# tunnel mpls traffic-eng priority 0 0</p>	Configures the setup and reservation priority for an MPLS traffic engineering tunnel.
<b>Step 9</b>	<pre>tunnel mpls traffic-eng bandwidth [sub-pool   global] bandwidth</pre> <p><b>Example:</b> Router(config-if)# tunnel mpls traffic-eng bandwidth 100</p>	Configures the bandwidth required for an MPLS traffic engineering tunnel.
<b>Step 10</b>	<pre>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number}} [lockdown]</pre> <p><b>Example:</b> Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit identifier 1</p>	Configures a path option for an MPLS traffic engineering tunnel.
<b>Step 11</b>	<pre>tunnel mpls traffic-eng fast-reroute</pre> <p><b>Example:</b> Router(config-if)# tunnel mpls traffic-eng fast-reroute</p>	Enables an MPLS traffic engineering tunnel to use an established backup tunnel in the event of a link failure.

## Establishing a Backup Tunnel Around the Link to be Protected

To configure a backup tunnel around the link you want to protect (R2–R3 in [Figure 1](#)), perform the following steps on the router that begins the link (R2 in [Figure 1](#)).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip unnumbered** *type number*
5. **tunnel destination** *A.B.C.D*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
8. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*}} [**lockdown**]
9. **ip explicit-path** {**name** *word* | **identifier** *number*} [{**enable** | **disable**}]
10. **next-address** *n.n.n.n*

### 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> [ <i>name-tag</i> ]  <b>Example:</b> Router(config)# interface Tunnel1000	Creates a tunnel interface and enters interface configuration mode.
Step 4	<b>ip unnumbered</b> <i>type number</i>  <b>Example:</b> Router(config-if)# ip unnumbered loopback0	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 5	<b>tunnel destination</b> <i>A.B.C.D</i>  <b>Example:</b> Router(config-if)# tunnel destination 25.1.1.1	Specifies the destination of a tunnel interface.

	Command or Action	Purpose
Step 6	<b>tunnel mode mpls traffic-eng</b>  <b>Example:</b> Router(config-if)# tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.
Step 7	<b>tunnel mpls traffic-eng priority</b> <i>setup-priority</i> [ <i>hold-priority</i> ]  <b>Example:</b> Router(config-if)# tunnel mpls traffic-eng priority 0 0	Configures the setup and reservation priority for an MPLS traffic engineering tunnel.
Step 8	<b>tunnel mpls traffic-eng path-option</b> <i>number</i> { <b>dynamic</b>   <b>explicit</b> { <i>name path-name</i>   <i>path-number</i> }} [ <b>lockdown</b> ]  <b>Example:</b> Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit identifier 2	Configures a path option for an MPLS traffic engineering tunnel.
Step 9	<b>ip explicit-path</b> { <i>name word</i>   <b>identifier</b> <i>number</i> } [{ <b>enable</b>   <b>disable</b> }]  <b>Example:</b> Router(config-if)# ip explicit-path identifier 2 enable	Enters the subcommand mode for IP explicit paths and creates or modifies the explicit path.
Step 10	<b>next-address</b> <i>n.n.n.n</i>  <b>Example:</b> Router(config-ip-explicit-path)# next-address 27.2.2.2	Specifies the next IP address in the explicit path.

## Configuring the Protected Link to Use the Backup Tunnel

To configure the protected link (R2–R3 in [Figure 1](#)) to use the backup tunnel, perform the following steps on the router whose outbound interface is the beginning of the link (R2 in that example).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip address** *a.b.c.d.e.f.g.h*
5. **mpls traffic-eng tunnels**
6. **mpls traffic-eng backup-path** **Tunnel** *interface*
7. **pos ais-shut**
8. **pos report lrdi**
9. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*]]



**Note** Steps 7 and Step 8 do not apply to the Cisco Series 10000 platform.

## 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 [name-tag]</i>  <b>Example:</b> Router(config)# interface pos	Moves configuration to the physical interface level, directing subsequent configuration commands to the specific physical interface identified by the <i>interface-id</i> . (In this release it is a POS interface.)
Step 4	<b>ip address</b> <i>a.b.c.d.e.f.g.h</i>  <b>Example:</b> Router(config-if)# ip address 160.2.2.1.255.255.255.0	Sets a primary IP address for this interface and a mask for the associated IP subnet.
Step 5	<b>mpls traffic-eng tunnels</b>  <b>Example:</b> Router(config-if)# mpls traffic-eng tunnels	Enables the MPLS traffic engineering tunnel feature on this physical interface.
Step 6	<b>mpls traffic-eng backup-path Tunnel</b> <i>interface</i>  <b>Example:</b> Router(config-if)# mpls traffic-eng backup-path Tunnel1000	Configures the physical interface to use a backup tunnel in the event of a detected failure on that physical interface.
Step 7	<b>pos ais-shut</b>  <b>Example:</b> Router(config-if)# pos ais-shut	Sends the alarm signal line (LAIS) when the POS interface is placed in an administrative shutdown state.
Step 8	<b>pos report lrdi</b>  <b>Example:</b> Router(config-if)# pos report lrdi	Permits selected SONET alarms to be logged to the console for a POS interface.
Step 9	<b>ip rsvp bandwidth</b> [ <i>interface-kbps [single-flow-kbps]</i> ]  <b>Example:</b> Router(config-if)# ip rsvp bandwidth 2480000 2480000	Enables RSVP for IP on an interface.

# Verifying that MPLS Traffic Engineering Fast Reroute Link Protection Has Been Enabled

Perform the following step to verify that MPLS traffic engineering Fast Reroute link protection has been enabled:

- Step 1** Use this command to verify that MPLS traffic engineering Fast Reroute link protection has been enabled:  
**show mpls traffic-eng fast-reroute database.**

```
Router# show mpls traffic-eng fast-reroute database 12.0.0.0
```

```
Tunnel head fast reroute information:
Prefix TunnelIn-labelOut intf/labelFRR intf/labelStatus
12.0.0.0/16Tu111Tun hdP00/0:UntaggedTu4000:16ready
12.0.0.0/16Tu449Tun hdP00/0:UntaggedTu4000:736ready
12.0.0.0/16Tu314Tun hdP00/0:UntaggedTu4000:757ready
12.0.0.0/16Tu313Tun hdP00/0:UntaggedTu4000:756ready
```

## Configuration Examples for MPLS Traffic Engineering Fast Reroute Link Protection

This section provides the following configuration examples:

- [Configuring a Tunnel for Fast Reroute Link Protection: Example, page 9](#)
- [Establishing a Backup Tunnel Around the Protected Link: Example, page 10](#)
- [Configuring the Protected Link to Use the Backup Tunnel: Example, page 10](#)

### Configuring a Tunnel for Fast Reroute Link Protection: Example

Enter the following commands at the tunnel headend (in [Figure 1](#) this is router R1):

```
interface Tunnel1
ip unnumbered loopback0
tunnel destination 25.1.1.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mode mpls traffic-eng priority 0 0
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng path-option 1 explicit identifier 1
tunnel mpls traffic-eng fast-reroute
```

## Establishing a Backup Tunnel Around the Protected Link: Example



### Note

Although you can route normal traffic on a backup tunnel, it is recommended that you do not; that is, do not use the autoroute or static routing functionality to direct traffic to the backup tunnel.

Enter the following commands on the router that begins the link you want to protect (in [Figure 1](#) this is router R2):

```
interface Tunnel1000
ip unnumbered loopback0
tunnel destination 27.2.2.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 0 0
tunnel mpls traffic-eng path-option 1 explicit identifier 2
ip explicit-path identifier 2 enable
next address n.n.n.n
next address n.n.n.n
next address 27.2.2.2
```

## Configuring the Protected Link to Use the Backup Tunnel: Example

Enter the following commands on the router that begins the protected link (R2 in [Figure 1](#)):

```
interface POS5/0
ip address 160.2.2.1 255.255.255.0
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
pos ais-shut
pos report lrdi
ip rsvp bandwidth 2480000 2480000
```

## Additional References

The following sections provide references related to MPLS Traffic Engineering Fast Reroute Link Protection.

## Related Documents

Related Topic	Document Title
Configuring Integrated IS-IS, Configuring OSPF	<i>Cisco IOS IP and IP Routing Configuration Guide</i> , Release 12.0
Integrated IS-IS commands, OSPF commands	<i>Cisco IOS IP and IP Routing Command Reference</i> , Release 12.0
Configuring RSVP	<i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , Release 12.0
IP RSVP commands	<i>Cisco IOS Quality of Service Solutions Command Reference</i> , Release 12.0
Multiprotocol Label Switching	<i>Cisco IOS Switching Services Configuration Guide</i> , Release 12.0
MPLS commands, Multiprotocol Label Switching	<i>Cisco IOS Switching Services Command Reference</i> , Release 12.0

## Standards

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

## MIBs

MIBs	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

RFCs	Title
RFC 1142	<i>IS-IS</i>
RFC 1195	<i>Use of OSI IS-IS for Routing in TCP/IP and Dual Environments</i>
RFC 2205	<i>Resource Reservation Protocol (RSVP)</i>
RFC 2328	<i>OSPF Version 2</i>
RFC 2370	<i>The OSPF Opaque LSA Option</i>
RFC 2702	<i>Requirements for Traffic Engineering Over MPLS</i>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

# Glossary

**backup LSP**—An LSP that may be used by the Fast Reroute procedure to temporarily repair one or more protected LSPs when a failure occurs. A backup LSP can be used to repair a protected LSP only if the backup LSP's destination is a router along the downstream path of the protected LSP.

**backup tunnel**—A Cisco IOS tunnel (software tunnelling interface) associated with a backup LSP. (This represents a temporary route to take in the event of a failure.)

**FRR**—Fast Reroute. The local forwarding of outbound traffic through an alternative traffic engineering tunnel when a link on the original tunnel fails.

**Group ID**—Two numerals enclosed in curly braces, where each numeral is a unique, Cisco IOS-assigned ID for, respectively, the physical and backup interfaces of a link-protected Fast-Reroute-enabled tunnel. For example, { 10,13 } is the Group ID for physical interface 10 and backup tunnel interface 13.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**IS-IS**—Intermediate System-to-Intermediate System. Link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric, to determine network topology.

**link protection**—Rerouting an LSP through a backup tunnel around a failed, “protected” link.

**LSP**—label switched path. A configured connection between two routers, in which MPLS is used to carry packets. A path created by the concatenation of one or more label switched hops, allowing a packet to be forwarded by swapping labels from an MPLS node to another MPLS node.

**midpoint**—A transit router for a given LSP.

**MPLS**—Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**MPLS global label allocation (GLA)**—Using one label space for all interfaces in the router. For example, label 100 coming in one interface is treated the same as label 100 coming in a different interface.

**OSPF**—Open Shortest Path First. A link-state, hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**protected LSP**—An LSP that is eligible for fast repair using the Fast Reroute feature.

**Rewrite**—An MPLS information block appended to the header of a packet for routing it through a traffic engineering tunnel. The rewrite stores much of the tunnel's forwarding state (output information).

**RSVP**—Resource Reservation Protocol. An IETF protocol used for signalling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

**SPF**—Shortest Path First. A routing algorithm that iterates on length-of-path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms. Sometimes called Dijkstra's algorithm.

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**TE**—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.



**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

