



# IP Security VPN Monitoring

---

The IP Security VPN Monitoring feature provides VPN session monitoring enhancements that will allow you to troubleshoot the Virtual Private Network (VPN) and monitor the end-user interface. Session monitoring enhancements include the following:

- Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file
- Summary listing of crypto session status
- Syslog notification for crypto session up or down status
- Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI)

## Feature History for IP Security VPN Monitoring

Release	Modification
12.3(4)T	This feature was introduced.

## 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 IP Security VPN Monitoring, page 2](#)
- [Restrictions for IP Security VPN Monitoring, page 2](#)
- [Information About IPSec VPN Monitoring, page 2](#)
- [How to Configure IP Security VPN Monitoring, page 4](#)
- [Configuration Examples for IP Security VPN Monitoring, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

## Prerequisites for IP Security VPN Monitoring

- You should be familiar with IPSec and encryption.
- Your router must support IPSec, and before using the IP Security VPN Monitoring feature, you must have configured IPSec on your router.

## Restrictions for IP Security VPN Monitoring

- You must be running Cisco IOS k8 or k9 crypto images on your router.

## Information About IPSec VPN Monitoring

To troubleshoot the IPSec VPN and monitor the end-user interface, you should understand the following concepts:

- [Background: Crypto Sessions, page 2](#)
- [Per-IKE Peer Description, page 2](#)
- [Summary Listing of Crypto Session Status, page 3](#)
- [Syslog Notification for Crypto Session Up or Down Status, page 3](#)
- [IKE and IPSec Security Exchange Clear Command, page 3](#)

## Background: Crypto Sessions

A crypto session is a set of IPSec connections (flows) between two crypto endpoints. If the two crypto endpoints use IKE as the keying protocol, they are IKE peers to each other. Typically, a crypto session consists of one IKE security association (for control traffic) and at least two IPSec security associations (for data traffic—one per each direction). There may be duplicated IKE security associations (SAs) and IPSec SAs or duplicated IKE SAs or IPSec SAs for the same session in the duration of rekeying or because of simultaneous setup requests from both sides.

## Per-IKE Peer Description

The Per-IKE Peer Description function allows you to enter a description of your choosing for an IKE peer. (Before Cisco IOS Release 12.3(4)T, you could use only the IP address or fully qualified domain name [FQDN] to identify the peer; there was no way to configure a description string.) The unique peer description, which can include up to 80 characters, can be used whenever you are referencing that particular IKE peer. To add the peer description, use the **description** command.



### Note

---

IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

---

The primary application of this description field is for monitoring purposes (for example, when using **show** commands or for logging [syslog messages]). The description field is purely informational (for example, it cannot act as a substitute for the peer address or FQDN when defining crypto maps).

## Summary Listing of Crypto Session Status

You can get a list of all the active VPN sessions by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by whom the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

You can also use the **show crypto session detail** variant of this command to obtain more detailed information about the sessions.

## Syslog Notification for Crypto Session Up or Down Status

The Syslog Notification for Crypto Session Up or Down Status function provides syslog notification every time the crypto session comes up or goes down.

The following is a sample syslog notification showing that a crypto session is up:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20  
Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

The following is a sample syslog notification showing that a crypto session is down:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10  
ivrf=name20 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

## IKE and IPsec Security Exchange Clear Command

In previous IOS versions, there was no single command to clear both IKE and IPsec connections (that is, SAs). Instead, you had to use the **clear crypto isakmp** command to clear IKE and the **clear crypto ipsec** command to clear IPsec. The new **clear crypto session** command allows you to clear both IKE and IPsec with a single command. To clear a specific crypto session or a subset of all the sessions (for example, a single tunnel to one remote site), you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, a front door VPN routing and forwarding (FVRF) name, or an inside VRF (IVRF) name. Typically, the remote IP address will be used to specify a single tunnel to be deleted.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPsec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be cleared. If you do not provide a parameter when you use the **clear crypto session** command, all IPsec SAs and IKE SAs that are in the router will be deleted.

# How to Configure IP Security VPN Monitoring

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional.

- [Adding the Description of an IKE Peer, page 4](#) (optional)
- [Verifying Peer Descriptions, page 5](#) (optional)
- [Clearing a Crypto Session, page 5](#) (optional)

## Adding the Description of an IKE Peer

To add the description of an IKE peer to an IPsec VPN session, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer {ip-address ip-address}**
4. **description**

### 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>crypto isakmp peer {ip-address ip-address}</b>  <b>Example:</b> Router (config)# crypto isakmp peer address 10.2.2.9	Enables an IPsec peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and enters ISAKMP peer configuration mode.
Step 4	<b>description</b>  <b>Example:</b> Router (config-isakmp-peer)# description connection from site A	Adds a description for an IKE peer.

## Verifying Peer Descriptions

To verify peer descriptions, use the **show crypto isakmp peer** command.

### SUMMARY STEPS

1. **enable**
2. **show crypto isakmp peer**

### 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>show crypto isakmp peer</b>  <b>Example:</b> Router# show crypto isakmp peer	Displays peer descriptions.

## Examples

The following output example verifies that the description “connection from site A” has been added for IKE peer 10.2.2.9:

```
Router# show crypto isakmp peer

Peer: 10.2.2.9 Port: 500
Description: connection from site A
flags: PEER_POLICY
```

When the peer at address 10.2.2.9 connects and the session comes up, the syslog status will be shown as follows:

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection from site A Id: ezvpn
```

## Clearing a Crypto Session

To clear a crypto session, use the **clear crypto session** command from the router command line. No configuration statements are required in the configuration file to use this command.

### SUMMARY STEPS

1. **enable**
2. **clear crypto session**

## 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>clear crypto session</code>  <b>Example:</b> Router# clear crypto session	Deletes crypto sessions (IPSec and IKE SAs).

## Configuration Examples for IP Security VPN Monitoring

This section provides the following configuration example:

- [show crypto session Command Output: Examples, page 6](#)

### show crypto session Command Output: Examples

The following is sample output for the `show crypto session` output without the `detail` keyword:

```
Router# show crypto session

Crypto session current status

Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
  IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
  IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
    Active SAs: 2, origin: crypto map
```

The following is sample output using the `show crypto session` command and the `detail` keyword:

```
Router# show crypto session detail

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
  Desc: this is my peer at 10.1.1.3:500 Green
  Phase1_id: 10.1.1.3
  IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
    Capabilities:(none) connid:3 lifetime:22:03:24
  IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
    Active SAs: 0, origin: crypto map
    Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
  IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
    Active SAs: 4, origin: crypto map
    Inbound: #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
    Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949
```

# Additional References

The following sections provide references related to IP Security VPN Monitoring.

## Related Documents

Related Topic	Document Title
IP security, encryption, and IKE	“ <a href="#">IP Security and Encryption</a> ” section of the <i>Cisco IOS Security Configuration Guide</i>
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T

## Standards

Standards	Title
No new or modified standards are supported by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported 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
No new or modified RFCs are supported by this feature.	—

## 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>

# Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

## New Commands

- **clear crypto session**
- **description (isakmp peer)**
- **show crypto isakmp peer**
- **show crypto session**

# clear crypto session

To delete crypto sessions (IP Security [IPSec] and Internet Key Exchange [IKE] security associations [SAs]), use the **clear crypto session** command in privileged EXEC mode.

```
clear crypto session [local ip-address [port local-port]] [remote ip-address [port remote-port]] |
[fvr vrf-name] [ivr vrf-name]
```

## Syntax Description

<b>local</b> <i>ip-address</i>	(Optional) Clears crypto sessions for a local crypto endpoint. <ul style="list-style-type: none"> <li>The <i>ip-address</i> is the IP address of the local crypto endpoint.</li> </ul>
<b>port</b> <i>local-port</i>	(Optional) IKE port of the local endpoint. The <i>local-port</i> value can be 1 through 65535. The default value is 500.
<b>remote</b> <i>ip-address</i>	(Optional) Clears crypto sessions for a remote IKE peer. <ul style="list-style-type: none"> <li>The <i>ip-address</i> is the IP address of the remote IKE peer.</li> </ul>
<b>port</b> <i>remote-port</i>	(Optional) IKE port of the remote endpoint to be deleted. The <i>remote-port</i> value can be from 1 through 65535. The default value is 500.
<b>fvr</b> <i>vrf-name</i>	(Optional) Clears a front door virtual routing and forwarding (FVRF) session.
<b>ivr</b> <i>vrf-name</i>	(Optional) Clears an inside VRF (IVRF) session.

## Defaults

If the **clear crypto session** command is entered without any keywords, all existing sessions will be deleted. The IPSec SAs will be deleted first, then the IKE SAs. Port default values are 500.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(4)T	This command was introduced.

## Usage Guidelines

To clear a specific crypto session or a subset of all the sessions, you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, a FVRF name, or an IVRF name.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPSec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be deleted.

## Examples

The following example shows that all crypto sessions will be deleted:

```
Router# clear crypto session
```

The following example shows that the crypto session of the FVRF named “blue” will be deleted:

```
Router# clear crypto session fvr blue
```

■ **clear crypto session**

The following example shows that the crypto sessions of the FVRF “blue” and the IVRF session “green” will be deleted:

```
Router# clear crypto session fvrf blue ivrf green
```

The following example shows that the crypto sessions of the local endpoint 10.1.1.1 and remote endpoint 10.2.2.2 will be deleted. The local endpoint port is 5, and the remote endpoint port is 10.

```
Router# clear crypto session local 10.1.1.1 port 5 remote 10.2.2.2 port 10
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>description</b>	Adds a description for an IKE peer.
<b>show crypto isakmp peer</b>	Displays peer descriptions.
<b>show crypto session</b>	Displays status information for active crypto sessions in a router.

## description (isakmp peer)

To add the description of an Internet Key Exchange (IKE) peer, use the **description** command in ISAKMP peer configuration mode. To delete the description, use the **no** form of this command.

**description** *line-of-description*

**no description** *line-of-description*

### Syntax Description

<i>line-of-description</i>	Description given to an IKE peer.
----------------------------	-----------------------------------

### Defaults

No default behavior or values

### Command Modes

ISAKMP peer configuration

### Command History

Release	Modification
12.3(4)T	This command was introduced.

### Usage Guidelines

IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

### Examples

The following example shows that the description “connection from site A” has been added for an IKE peer:

```
Router# crypto isakmp peer address 10.2.2.9
Router (config-isakmp-peer)# description connection from site A
```

### Related Commands

Command	Description
<b>clear crypto session</b>	Deletes crypto sessions (IPSec and IKE SAs).
<b>show crypto isakmp peer</b>	Displays peer descriptions.
<b>show crypto session</b>	Displays status information for active crypto sessions in a router.

# show crypto isakmp peer

To display peer descriptions, use the **show crypto isakmp peer** command in privileged EXEC mode.

**show crypto isakmp peer**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(4)T	This command was introduced.

**Examples** The following output example shows information about the peer named “This-is-another-peer-at-10-1-1-3”:

```
Router# show crypto isakmp peer
```

```
Peer: 10.1.1.3 Port: 500
Description: This-is-another-peer-at-10-1-1-3
Phase1 id: 10.1.1.3
```

[Table 1](#) describes the significant fields shown in the display.

**Table 1** *show crypto isakmp peer Field Descriptions*

Field	Description
Phase1 id	Internet Key Exchange (IKE) ID

Related Commands	Command	Description
	<b>clear crypto session</b>	Deletes crypto sessions (IPSec and IKE) SAs.
	<b>description</b>	Adds a description for an IKE peer.
	<b>show crypto session</b>	Displays status information for active crypto sessions in a router.

# show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in privileged EXEC mode.

```
show crypto session [detail] | [local ip-address [port local-port] [remote ip-address [port remote-port]] [detail]] | [fvfr vrf-name] [ivrf vrf-name] [detail]
```

Syntax Description		
<b>detail</b>	(Optional) Provides more detailed information about the session, such as the capability of the Internet Key Exchange (IKE) security association (SA), connection ID, remaining lifetime of the IKE SA, inbound or outbound encrypted or decrypted packet number of the IP Security (IPSec) flow, dropped packet number, and kilobyte-per-second lifetime of the IPSec SA.	
<b>local ip-address</b>	(Optional) Displays status information about crypto sessions of a local crypto endpoint.	<ul style="list-style-type: none"> <li>The <i>ip-address</i> value is the IP address of the local crypto endpoint.</li> </ul>
<b>port local-port</b>	(Optional) Port of the local crypto endpoint.	<ul style="list-style-type: none"> <li>The <i>local-port</i> value can be 1 through 65535. The default value is 500.</li> </ul>
<b>remote ip-address</b>	(Optional) Displays status information about crypto sessions of a remote session.	<ul style="list-style-type: none"> <li>The <i>ip-address</i> value is the IP address of the remote crypto endpoint.</li> </ul>
<b>port remote-port</b>	(Optional) Displays status information about crypto sessions of a remote crypto endpoint.	<ul style="list-style-type: none"> <li>The <i>remote-port</i> value can be 1 through 65535. The default value is 500.</li> </ul>
<b>fvfr vrf-name</b>	(Optional) Displays status information about the front door virtual routing and forwarding (FVRF) session.	
<b>ivrf vrf-name</b>	(Optional) Displays status information about the inside VRF (IVRF) session.	

**Defaults** If the **show crypto session** command is entered without any keywords, all existing sessions will be displayed. Port default values are 500.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(4)T	This command was introduced.

**Usage Guidelines**

You can get a list of all the active Virtual Private Network (VPN) sessions and of the IKE and IPSec SAs for each VPN session by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by whom the IPSec SAs are created
- IPSec SAs serving the flows of a session

Multiple IKE or IPSec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPSec SAs that are serving the flows of the session.

**Examples**

The following example shows active VPN sessions:

```
Router# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Ethernet1/0
Session status: UP-NO-IKE
Peer: 10.2.80.179/500 fvrf: (none) ivrf: (none)
  Desc: My-manual-keyed-peer
  Phase1_id: 10.2.80.179
  IPSEC FLOW: permit ip host 10.2.80.190 host 10.2.80.179
    Active SAs: 4, origin: manual-keyed crypto map
    Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Ethernet1/2
Session status: DOWN
Peer: 10.1.1.1/500 fvrf: (none) ivrf: (none)
  Desc: SJC24-2-VPN-Gateway
  Phase1_id: 10.1.1.1
  IPSEC FLOW: permit ip host 10.2.2.3 host 10.2.2.2
    Active SAs: 0, origin: crypto map
    Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
  IPSEC FLOW: permit ip 10.2.0.0/255.255.0.0 10.4.0.0/255.255.0.0
    Active SAs: 0, origin: crypto map
    Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Serial2/0.17
Session status: UP-ACTIVE
Peer: 10.1.1.5/500 fvrf: (none) ivrf: (none)
  Desc: (none)
  Phase1_id: 10.1.1.5
  IKE SA: local 10.1.1.5/500 remote 10.1.1.5/500 Active
    Capabilities:(none) connid:1 lifetime:00:59:51
  IPSEC FLOW: permit ip host 10.1.1.5 host 10.1.2.5
    Active SAs: 2, origin: dynamic crypto map
    Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 20085/171
    Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 20086/171
```

Table 2 describes the significant fields shown in the display.

**Table 2** *show crypto isakmp peer Field Descriptions*

Field	Description
Interface	Interface to which the crypto session is related.
Session status	Current status of the crypto (VPN) sessions. See Table 3 for the status of the IKE SA, IPsec SA, and tunnel as shown in the display.
IKE SA	Information is provided about the IKE SA, such as local and remote address and port, SA status, SA capabilities, crypto engine connection ID, and remaining lifetime of the IKE SA.
IPSEC FLOW	A snapshot of information about the IPsec-protected traffic flow, such as what the flow is (for example, “permit ip host 10.1.1.5 host 10.1.2.5”); how many IPsec SAs there are; the origin of the SA, such as manual keyed, dynamic, or static crypto map; the number of encrypted or decrypted packets or dropped packets; and the IPsec SA remaining lifetime in kilobytes per second.

Table 3 provides an explanation of the current status of the VPN sessions shown in the display.

**Table 3** *Current Status of the VPN Sessions*

IKE SA	IPsec SA	Tunnel Status
Exist, active	Exist (flow exists)	UP-ACTIVE
Exist, active	None (flow exists)	UP-IDLE
Exist, active	None (no flow)	UP-IDLE
Exist, inactive	Exist (flow exists)	UP-NO-IKE
Exist, inactive	None (flow exists)	DOWN-NEGOTIATING
Exist, inactive	None (no flow)	DOWN-NEGOTIATING
None	Exist (flow exists)	UP-NO-IKE
None	None (flow exists)	DOWN
None	None (no flow)	DOWN



**Note**

IPsec flow may not exist if a dynamic crypto map is being used.

**Related Commands**

Command	Description
<b>clear crypto session</b>	Deletes crypto sessions (IPsec and IKE SAs).
<b>description</b>	Adds a description for an IKE peer.
<b>show crypto isakmp peer</b>	Displays peer descriptions.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.