



Integrating NAT with MPLS VPNs

Network Address Translation (NAT) Integration with MPLS VPNs feature allows multiple Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) to be configured on a single device to work together. NAT can differentiate which MPLS VPN it receives IP traffic from even if the MPLS VPNs are all using the same IP addressing scheme. This enhancement enables multiple MPLS VPN customers to share services while ensuring that each MPLS VPN is completely separate from the other.

Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Integrating NAT with MPLS VPNs”](#) section on page 12.

Contents

- [Prerequisites for Integrating NAT with MPLS VPNs, page 1](#)
- [Restrictions for Integrating NAT with MPLS VPNs, page 2](#)
- [Information About Integrating NAT with MPLS VPNs, page 2](#)
- [How to Integrate NAT with MPLS VPNs, page 3](#)
- [Configuration Examples for Integrating NAT with MPLS VPNs, page 10](#)
- [Where to Go Next, page 11](#)
- [Additional References, page 12](#)

Prerequisites for Integrating NAT with MPLS VPNs

- Before performing the tasks in this module, you should be familiar with the concepts described in the [“Configuring NAT for IP Address Conservation”](#) module.



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

© 2007 Cisco Systems, Inc. All rights reserved.

- All access lists required for use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the “*IP Access List Sequence Numbering*” document at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm>



Note If you specify an access list to use with a NAT command, NAT does not support the commonly used **permit ip any any** command in the access list.

Restrictions for Integrating NAT with MPLS VPNs

Inside VPN to VPN with NAT is not supported.

Information About Integrating NAT with MPLS VPNs

To integrate NAT with MPLS VPNs, you should understand the following concepts:

- [Benefits of NAT Integration with MPLS VPNs, page 2](#)
- [Implementation Options for Integrating Nat with MPLS VPNs, page 2](#)
- [Scenarios for Implementing NAT on the PE Router, page 2](#)

Benefits of NAT Integration with MPLS VPNs

MPLS service providers would like to provide value-added services such as Internet connectivity, domain name servers (DNS), and voice over IP (VoIP) service to their customers. The providers require that their customers; IP addresses be different when reaching the services. Because MPLS VPN allows customers to use overlapped IP addresses in their networks, NAT must be implemented to make the services possible.

Implementation Options for Integrating Nat with MPLS VPNs

There are two approaches to implementing NAT in the MPLS VPN network. NAT can be implemented on the customer edge (CE) router, which is already supported by NAT, or it can be implemented on a provider edge (PE) router. The NAT Integration with MPLS VPNs feature enables the implementation of NAT on a PE router in an MPLS cloud.

Scenarios for Implementing NAT on the PE Router

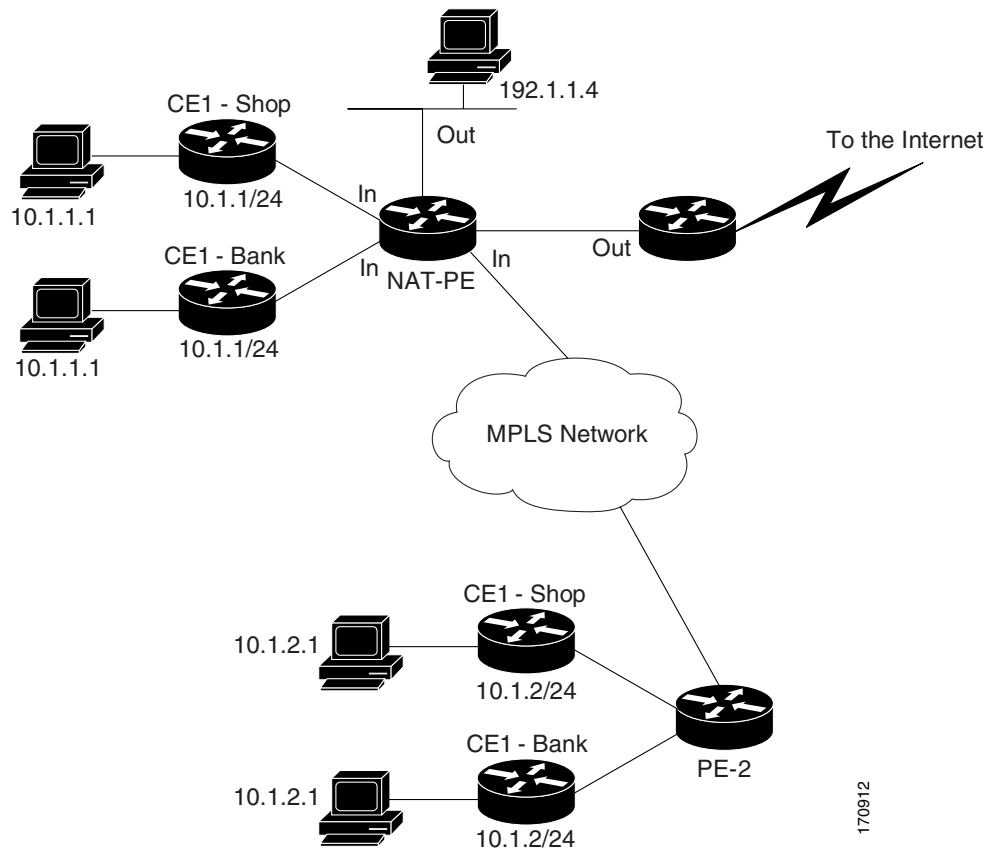
NAT could be implemented on the PE router in the following scenarios:

- Service point—Shared access can be from a generic interface or from a VPN interface.
- NAT point—NAT can be configured on the PE router that is directly connected to the shared access gateway, or on the PE router that is not directly connected to the shared access gateway.

- **NAT interface**—The shared access gateway interface most often is configured as the outside interface of NAT. The inside interface of NAT can be either the PE-CE interface of a VPN, the interface to the MPLS backbone, or both. The shared access gateway interface can also be configured as the inside interface.
- **Routing type**—Common service can be Internet connectivity or a common server. For Internet connectivity, a default route should be propagated to all the VPN customers that use the service. For common server access, a static or dynamically learned route should be propagated to the VPN customers.
- **NAT configuration**—NAT can have different configurations: static, dynamic, pool/interface overloading, and route-map.

Figure 1 shows a typical NAT integration with MPLS VPNs. The PE router connected to the internet and centralized mail service is employed to do the address translation.

Figure 1 Typical NAT Integration with MPLS VPNs



How to Integrate NAT with MPLS VPNs

Perform one or more of the following tasks depending on the type of translation you wish to configure for your network:

- [Configuring Inside Dynamic NAT with MPLS VPNs, page 4](#) (optional)
- [Configuring Inside Static NAT with MPLS VPNs, page 6](#) (optional)

- [Configuring Outside Dynamic NAT with MPLS VPNs, page 7](#) (optional)
- [Configuring Outside Static NAT with MPLS VPNs, page 8](#) (optional)

Configuring Inside Dynamic NAT with MPLS VPNs

Perform this task to configure your NAT PE router for dynamic translations to integrate with MPLS VPNs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip netmask netmask*
4. **ip nat** [**inside** | **outside**] **source** [**list** {*access-list-number* | *access-list-name*} | **route-map** *name*] [**interface** *type number* | **pool** *pool-name*] **vrf** *vrf-name* [**overload**]
5. Repeat Step 4 for all VPNs being configured.
6. **ip route vrf** *vrf-name prefix mask interface-type interface-number next-hop-address*
7. Repeat Step 6 for all VPNs being configured.
8. **exit**
9. **show ip nat translations vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip nat pool <i>name start-ip end-ip netmask netmask</i> Example: Router(config)# ip nat pool inside 2.2.2.10 2.2.2.10 netmask 255.255.255.0	Defines a pool of IP addresses for NAT.

	Command or Action	Purpose
Step 4	<pre>ip nat [inside outside] source [list {access-list-number / access-list-name} route-map name] [interface type number pool pool-name] vrf vrf-name [overload]</pre> <p>Example: Router(config)# ip nat inside source list 1 pool mypool vrf shop overload</p>	Allows NAT to be configured on a particular VPN.
Step 5	Repeat Step 4 for each VPN being configured	Allows NAT to be configured on a particular VPN.
Step 6	<pre>ip route vrf vrf-name prefix mask interface-type interface-number next-hop-address</pre> <p>Example: Router(config)# ip route vrf shop 0.0.0.0 0.0.0.0 ethernet 0 168.58.88.2</p>	Allows NAT to be configured on a particular VPN.
Step 7	Repeat Step 6 for each VPN being configured.	Allows NAT to be configured on a particular VPN.
Step 8	<pre>exit</pre> <p>Example: Router> exit</p>	Returns to privileged EXEC mode.
Step 9	<pre>show ip nat translations vrf vrf-name</pre> <p>Example: Router# show ip nat translations vrf shop</p>	(Optional) Displays the settings used by virtual routing/forwarding (VRF) table translations.

Configuring Inside Static NAT with MPLS VPNs

Perform this task to configure your NAT PE router for static translations to integrate with MPLS VPNs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat inside source {static {esp local-ip interface type number | local-ip global-ip}} [extendable | mapping-id map-id | no-alias | no-payload | redundancy group-name | route-map | vrf name]**
4. Repeat Step 3 for each VPN being configured.
5. **ip route vrf vrf-name prefix prefix mask next-hop-address global**
6. Repeat Step 5 for each VPN being configured.
7. **exit**
8. **show ip nat translations vrf vrf-name**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip nat inside source {static {esp local-ip interface type number local-ip global-ip}} [extendable mapping-id map-id no-alias no-payload redundancy group-name route-map vrf name] Example: Router(config)# ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop	Enables inside static translation on the VRF.
Step 4	Repeat Step 3 for each VPN being configured.	Enables inside static translation on the VRF.
Step 5	ip route vrf vrf-name prefix prefix mask next-hop-address global Example: Router(config)# ip route vrf shop 0.0.0.0 0.0.0.0 168.58.88.2 global	Allows the route to be shared by several customers.
Step 6	Repeat Step 5 for each VPN being configured.	Allows the route to be shared by several customers.

	Command or Action	Purpose
Step 7	exit Example: Router> exit	Returns to privileged EXEC mode.
Step 8	show ip nat translations vrf vrf-name Example: Router# show ip nat translations vrf shop	(Optional) Displays the settings used by VRF translations.

Configuring Outside Dynamic NAT with MPLS VPNs

Perform this step to configure your NAT PE router for dynamic outside translations to integrate with MPLS VPNs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat pool outside global-ip local-ip netmask netmask**
4. **ip nat inside source static local-ip global-ip vrf vrf-name**
5. Repeat Step 4 for each VRF being configured.
6. **ip nat outside source static global-ip local-ip vrf vrf-name**
7. **exit**
8. **show ip nat translations vrf vrf-name**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip nat pool outside global-ip local-ip netmask netmask Example: Router(config)# ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.00	Allows the configured VRF to be associated with the NAT translation rule.

	Command or Action	Purpose
Step 4	<pre>ip nat inside source static local-ip global-ip vrf vrf-name</pre> <p>Example: Router(config)# ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop </p>	Allows the route to be shared by several customers.
Step 5	Repeat Step 4 for each VRF being configured.	Allows the route to be shared by several customers.
Step 6	<pre>ip nat outside source static global-ip local-ip vrf vrf-name</pre> <p>Example: Router(config)# ip nat outside source static 168.58.88.2 4.4.4.1 vrf shop </p>	Enables NAT translation of the outside source address.
Step 7	<pre>exit</pre> <p>Example: Router> exit </p>	Returns to privileged EXEC mode.
Step 8	<pre>show ip nat translations vrf vrf-name</pre> <p>Example: Router# show ip nat translations vrf shop </p>	(Optional) Displays the settings used by VRF translations.

Configuring Outside Static NAT with MPLS VPNs

Perform this task to configure your NAT PE router for static outside translations to integrate with MPLS VPNs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat pool inside** *global-ip local-ip netmask netmask*
4. Repeat Step 3 for each pool being configured.
5. **ip nat inside source list** *access-list-number pool pool-name vrf vrf-name*
6. Repeat Step 5 for each pool being configured.
7. **ip nat outside source static** *global-ip local-ip vrf vrf-name*
8. Repeat Step 7 for all VPNs being configured.
9. **exit**
10. **show ip nat translations vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	configure { terminal memory network } Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip nat pool inside <i>global-ip local-ip netmask netmask</i> Example: Router(config)# ip nat pool inside1 2.2.1.1 2.2.1.254 netmask 255.255.255.0	Allows the configured VRF to be associated with the NAT translation rule.
Step 4	Repeat Step 3 for each pool being configured.	Allows the configured VRF to be associated with the NAT translation rule.
Step 5	ip nat inside source list <i>access-list-number pool pool-name vrf vrf-name</i> Example: Router(config)# ip nat inside source list 1 pool inside2 vrf shop	Allows the route to be shared by several customers.
Step 6	Repeat Step 5 for each pool being configured.	Defines the access list.
Step 7	ip nat outside source static <i>global-ip local-ip vrf vrf-name</i> Example: Router(config)# ip nat outside source static 168.58.88.2 4.4.4.1 vrf shop	Allows the route to be shared by several customers.
Step 8	Repeat Step 7 for all VPNs being configured.	Allows the route to be shared by several customers.
Step 9	exit Example: Router> exit	Returns to privileged EXEC mode.
Step 10	show ip nat translations vrf <i>vrf-name</i> Example: Router# show ip nat translations vrf shop	(Optional) Displays the settings used by VRF translations.

Configuration Examples for Integrating NAT with MPLS VPNs

This section provides the following configuration examples:

- [Configuring Inside Dynamic NAT with MPLS VPNs: Example, page 10](#)
- [Configuring Outside Dynamic NAT with MPLS VPNs: Example, page 11](#)
- [Configuring Inside Static NAT with MPLS VPNs: Example, page 10](#)
- [Configuring Outside Static NAT with MPLS VPNs: Example, page 11](#)

Configuring Inside Dynamic NAT with MPLS VPNs: Example

The following example shows configuring inside Dynamic NAT with MPLS VPNs.

```
!
ip nat pool inside 2.2.2.10 2.2.2.10 netmask 255.255.255.0
ip nat inside source list 1 pool inside vrf bank overload
ip nat inside source list 1 pool inside vrf park overload
ip nat inside source list 1 pool inside vrf shop overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 Ethernet1/3 168.58.88.2
ip route vrf bank 0.0.0.0 0.0.0.0 Ethernet1/3 168.58.88.2
ip route vrf park 0.0.0.0 0.0.0.0 Ethernet1/3 168.58.88.2
!
access-list 1 permit 192.168.0.0 0.0.255.255
```

Configuring Inside Static NAT with MPLS VPNs: Example

The following example shows configuring inside static NAT with MPLS VPNs.

```
!
ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop
ip nat inside source static 192.168.122.49 2.2.2.2 vrf shop
ip nat inside source static 192.168.121.113 2.2.2.3 vrf bank
ip nat inside source static 192.168.22.49 2.2.2.4 vrf bank
ip nat inside source static 192.168.121.113 2.2.2.5 vrf park
ip nat inside source static 192.168.22.49 2.2.2.6 vrf park
ip nat inside source static 192.168.11.1 2.2.2.11 vrf shop
ip nat inside source static 192.168.11.3 2.2.2.12 vrf shop
ip nat inside source static 140.48.5.20 2.2.2.13 vrf shop
!
ip route 2.2.2.1 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.2 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.3 255.255.255.255 Serial12/1.1 192.168.121.113
ip route 2.2.2.4 255.255.255.255 Serial12/1.1 192.168.121.113
ip route 2.2.2.5 255.255.255.255 FastEthernet0/0 192.168.121.113
ip route 2.2.2.6 255.255.255.255 FastEthernet0/0 192.168.121.113
ip route 2.2.2.11 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.12 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.13 255.255.255.255 Ethernet1/0 192.168.121.113
```

Configuring Outside Dynamic NAT with MPLS VPNs: Example

The following example shows configuring outside dynamic NAT with MPLS VPNs.

```
!  
ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.0  
ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop  
ip nat inside source static 192.168.122.49 2.2.2.2 vrf shop  
ip nat inside source static 192.168.121.113 2.2.2.3 vrf bank  
ip nat inside source static 192.168.22.49 2.2.2.4 vrf bank  
ip nat inside source static 192.168.121.113 2.2.2.5 vrf park  
ip nat inside source static 192.168.22.49 2.2.2.6 vrf park  
ip nat outside source list 1 pool outside  
!
```

Configuring Outside Static NAT with MPLS VPNs: Example

The following example shows configuring outside static NAT with MPLS VPNs.

```
!  
ip default-gateway 10.1.15.1  
ip nat pool inside1 2.2.1.1 2.2.1.254 netmask 255.255.255.0  
ip nat pool inside2 2.2.2.1 2.2.2.254 netmask 255.255.255.0  
ip nat pool inside3 2.2.3.1 2.2.3.254 netmask 255.255.255.0  
ip nat inside source list 1 pool inside2 vrf bank  
ip nat inside source list 1 pool inside3 vrf park  
ip nat inside source list 1 pool inside1 vrf shop  
ip nat outside source static 168.58.88.2 4.4.4.1 vrf bank  
ip nat outside source static 18.68.58.1 4.4.4.2 vrf park  
ip nat outside source static 168.58.88.1 4.4.4.3 vrf shop  
ip classless  
ip route 192.170.10.0 255.255.255.0 Ethernet1/0 192.168.121.113  
ip route 192.170.11.0 255.255.255.0 Serial2/1.1 192.168.121.113  
ip route 192.170.12.0 255.255.255.0 FastEthernet0/0 192.168.121.113  
ip route vrf shop 0.0.0.0 0.0.0.0 168.58.88.2 global  
ip route vrf bank 0.0.0.0 0.0.0.0 168.58.88.2 global  
ip route vrf park 0.0.0.0 0.0.0.0 168.58.88.2 global  
no ip http server  
!  
access-list 1 permit 192.168.0.0 0.0.255.255
```

Where to Go Next

- To learn about Network Address Translation and configure NAT for IP address conservation, see the “Configuring NAT for IP Address Conservation” module.
- To verify, monitor, and maintain NAT, see the “Monitoring and Maintaining NAT” module.
- To use NAT with application level gateways, see the “Using Application Level Gateways with NAT” module.
- To configure NAT for high availability, see the “Configuring NAT for High Availability” module.

Additional References

The following sections provide references related to NAT.

Related Documents

Related Topic	Document Title
NAT commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS IP Addressing Services Command Reference
NAT high availability	“Configuring NAT for High Availability” module
Application Level Gateways	“Using Application Level Gateways with NAT”
Maintain and monitor NAT	“Monitoring and Maintaining NAT” module
IP Address Conservation	“Configuring NAT for IP Address Conservation” module

Standards

Standards	Title
None	

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> None 	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs ¹	Title
RFC 2547	BGP/MPLS VPNs

1. Not all supported RFCs are listed.

Feature Information for Integrating NAT with MPLS VPNs

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.1(13) T or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the “Configuring Network Address Translation Features Roadmap.”

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 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.

**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 Integrating NAT with MPLS VPNs

Feature Name	Releases	Feature Configuration Information
Network Address Translation (NAT) Integration with MPLS VPNs feature	12.1(13)T	<p>This feature allows multiple Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) to be configured on a single device to work together.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> “Information About Integrating NAT with MPLS VPNs” section on page 2 “How to Integrate NAT with MPLS VPNs” section on page 3

Technical Assistance

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

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)

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.

© 2007 Cisco Systems, Inc. All rights reserved.