



NAT Integration with MPLS VPNs

The NAT Integration with MPLS VPNs feature allows multiple MPLS 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.

Feature Specifications for NAT Integration with MPLS VPNs

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To obtain updated information about platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. In the release section, you can compare releases side by side to display both the features unique to each software release and the features that releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Contents

- [Restrictions for NAT Integration with MPLS VPNs, page 2](#)
- [Information About NAT Integration with MPLS VPNs, page 2](#)
- [How to Configure NAT Integration with MPLS VPNs, page 4](#)
- [Additional References, page 11](#)
- [Command Reference, page 12](#)

Restrictions for NAT Integration with MPLS VPNs

Inside VPN to VPN with NAT is not supported.

Information About NAT Integration with MPLS VPNs

Before you configure NAT integration with MPLS VPNs, you should understand the following concepts:

- [Benefits of NAT Integration 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 VoIP service to their customers. This requires 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.

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

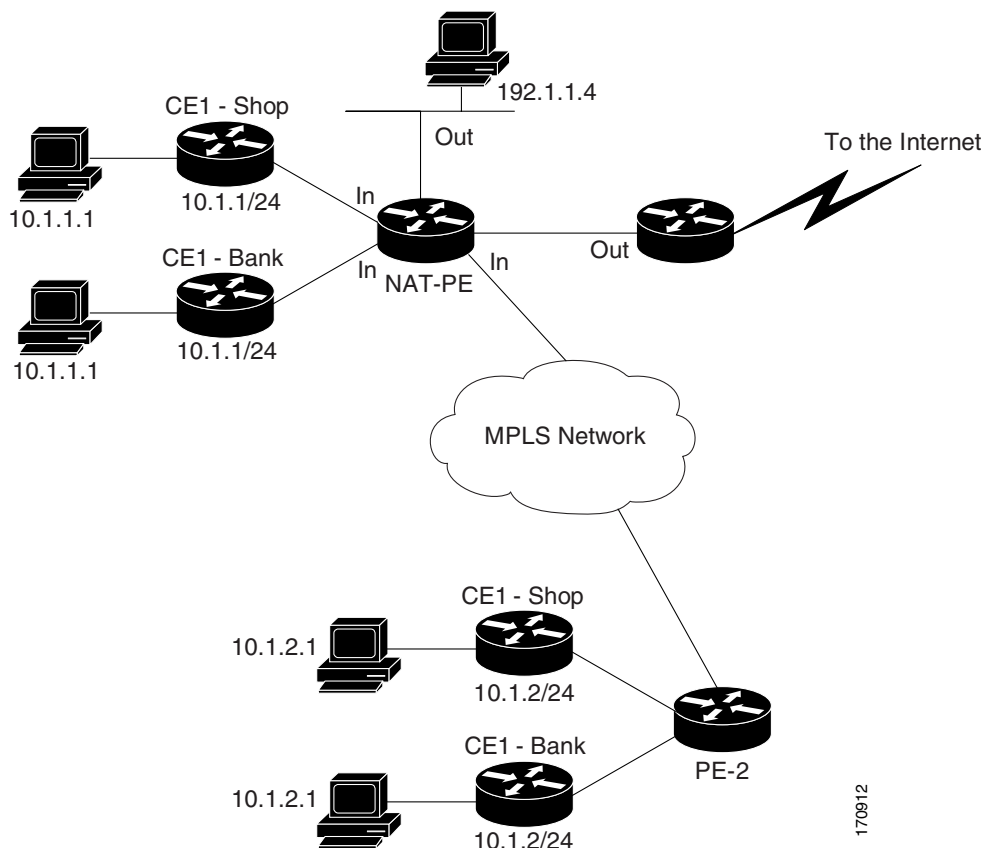
NAT could be implemented on the PE route in the following scenarios:

- 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 Configure NAT Integration with MPLS VPNs

The following sections describe configuration tasks for NAT Integration with MPLS VPNs. The tasks you perform depends on whether you are configuring inside or outside networks and whether you chose static or dynamic NAT.

- [Configuring Inside Dynamic NAT with MPLS VPNs, page 4](#)
- [Configuring Inside Static NAT with MPLS VPNs Example, page 9](#)
- [Configuring Outside Dynamic NAT with MPLS VPNs Example, page 10](#)
- [Configuring Outside Static NAT with MPLS VPNs Example, page 10](#)

Configuring Inside Dynamic NAT with MPLS VPNs

To configure your NAT-PE router for dynamic translations to integrate with MPLS VPNs, perform the following steps in the order shown:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
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 next-hop-address*
7. Repeat Step 6 for all VPNs being configured.
8. **access-list** *access-list-number permit ip-address mask*

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 memory network }	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<pre>ip nat pool name start-ip end-ip netmask netmask</pre> <p>Example: Router(config)# ip nat pool inside 2.2.2.10 2.2.2.10 netmask 255.255.255.0</p>	Defines a pool of IP addresses for NAT.
Step 4	<pre>ip nat inside source {list {access-list-number access-list-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 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>access-list access-list-number permit ip-address mask</pre> <p>Example: Router(config)# access-list 2 permit 10.1.1.0 0.0.0.255</p>	Defines the access list.

Configuring Inside Static NAT with MPLS VPNs

To configure your NAT PE router for static translations to integrate with MPLS VPNs, perform the following steps in the order shown.

SUMMARY STEPS

1. **enable**
2. **configure** {terminal | memory | network }
3. **ip nat inside source static** ip-address ip-address vrf vrf-name
4. Repeat Step 3 for each pool being configured.
5. **ip route vrf** vrf-name prefix prefix mask next-hop-address **global**
6. Repeat Step 5 for each VPN being configured.

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 inside source static <i>local-ip</i> <i>global-ip</i> vrf <i>vrf-name</i> global 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 <i>vrf-name</i> prefix <i>prefix mask</i> <i>next-hop-address</i> 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.

Configuring Outside Dynamic NAT with MPLS VPNs

To configure your NAT PE router for static outside translations to integrate with MPLS VPNs, perform the following steps in the order shown.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **nip 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*

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 outside <i>global-ip local-ip netmask netmask</i> Example: Router(config)# ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.0	Allows the configured VRF to be associated with the NAT translation rule.
Step 4	ip nat inside source static <i>local-ip global-ip vrf vrf-name</i> Example: Router(config)# ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop	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	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	Enables NAT translation of the outside source address.

Configuring Outside Static NAT with MPLS VPNs

To configure your NAT PE router for static outside translations to integrate with MPLS VPNs, perform the following steps in the order shown.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
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.

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 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 VPN 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.

Verifying NAT with MPLS VPNs

To verify your configuration, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **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	show ip nat translations vrf vrf-name Example: Router# show ip nat translations vrf shop	Displays the settings used by VRF translations.

Configuration Examples for NAT with MPLS VPNs

This section provides the following configuration examples:

- [Configuring Inside Dynamic NAT with MPLS VPNS Example, page 9](#)
- [Configuring Outside Dynamic NAT with MPLS VPNs Example, page 10](#)
- [Configuring Inside Static NAT with MPLS VPNs Example, page 9](#)
- [Configuring Outside Static NAT with MPLS VPNs Example, page 10](#)

Configuring Inside Dynamic NAT with MPLS VPNS Example

```
!
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

```
!
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 Serial2/1.1 192.168.121.113
ip route 2.2.2.4 255.255.255.255 Serial2/1.1 192.168.121.113
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

```

!
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

```

!
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

```

Additional References

For additional information related to Network Address Translation, refer to the following references:

[Related Documents, page 11](#)

[MIBs, page 11](#)

[RFCs, page 12](#)

[Technical Assistance, page 12](#)

Related Documents

Related Topic	Document Title
Additional NAT configuration tasks	The chapter “Configuring IP Addressing” in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2
Additional NAT commands	The chapter “IP Addressing Commands” in the <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> , Release 12.2

MIBs

MIBs ¹	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 2547	<i>BGP/MPLS VPNs</i>

1. Not all supported RFCs are listed.

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, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **debug ip nat**
- **ip nat inside source**
- **ip nat outside source**
- **show ip nat translations**

debug ip nat

To display information about IP packets translated by the IP Network Address Translation (NAT) feature, use the **debug ip nat** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip nat [access-list | detailed | h323 | pptp | sip | vrf]
```

```
no debug ip nat [access-list | detailed | h323 | pptp | sip | vrf]
```

Syntax Description

<i>access-list</i>	(Optional) The standard IP access list number. If the datagram is not permitted by the specified access list, the related debugging output is suppressed.
detailed	(Optional) Displays debug information in a detailed format.
h323	(Optional) Displays H.225 and H.245 protocol information.
pptp	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) information.
sip	(Optional) Displays Session Initiation Protocol (SIP) information.
vrf	(Optional) Displays VRF traffic-related information.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(5)T	This command was modified to include the h323 keyword.
12.2(8)T	This command was modified to include the sip keyword.
12.2(13)T	This command was modified to include the vrf keyword.

Usage Guidelines

The NAT feature reduces the need for unique, registered IP addresses. It can also save private network administrators from needing to renumber hosts and routers that do not conform to global IP addressing.

Use the **debug ip nat** command to verify the operation of the NAT feature by displaying information about every packet that is translated by the router. The **debug ip nat detailed** command generates a description of each packet considered for translation. This command also outputs information about certain errors or exceptional conditions, such as the failure to allocate a global address. To display messages related to the processing of H.225 signaling and H.245 messages, use the **debug ip nat h323** command. To display messages related to the processing of SIP messages, use the **debug ip nat sip** command. To display messages related to the processing of VRF messages, use the **debug ip nat vrf** command.

**Caution**

Because the **debug ip nat** command generates a substantial amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

Examples

The following is sample output from the **debug ip nat** command. In this example, the first two lines show the debugging output produced by a Domain Name System (DNS) request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. All Telnet packets, except for the first packet, were translated in the fast path, as indicated by the asterisk (*).

```
Router# debug ip nat
NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23325]
```

Table 1 describes the significant fields shown in the display.

Table 1 *debug ip nat Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature. An asterisk (*) indicates that the translation is occurring in the fast path. The first packet in a conversation always goes through the slow path (that is, it is process switched). The remaining packets go through the fast path if a cache entry exists.
s=192.168.1.95->172.31.233.209	Source address of the packet and how it is being translated.
d=172.31.2.132	Destination address of the packet.
[6825]	IP identification number of the packet. Might be useful in the debugging process to correlate with other packet traces from protocol analyzers.

The following is sample output from the **debug ip nat detailed** command. In this example, the first two lines show the debugging output produced by a DNS request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. In this example, the inside host 192.168.1.95 was assigned the global address 172.31.233.193.

```
Router# debug ip nat detailed
NAT: i: udp (192.168.1.95, 1493) -> (172.31.2.132, 53) [22399]
NAT: o: udp (172.31.2.132, 53) -> (172.31.233.193, 1493) [63671]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22400]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22002]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22401]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22402]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22060]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22071]
```

The following is sample output from the **debug ip nat h323** command. In this example, an H.323 call is established between two hosts, one host on the inside and the other one on the outside. The debug output displays the H.323 messages names that NAT recognizes and the embedded IP addresses contained in those messages.

```
Router# debug ip nat h323
NAT:H225:[0] processing a Setup message
NAT:H225:[0] found Setup sourceCallSignalling
NAT:H225:[0] fix TransportAddress addr=192.168.122.50 port=11140
NAT:H225:[0] found Setup fastStart
NAT:H225:[0] Setup fastStart PDU length:18
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC forward mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[0] Setup fastStart PDU length:29
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC reverse mediaChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16516
NAT:H245:[0] found OLC reverse mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[1] processing an Alerting message
NAT:H225:[1] found Alerting fastStart
NAT:H225:[1] Alerting fastStart PDU length:25
NAT:H245:[1] processing OpenLogicalChannel message, forward channe
```

Table 2 describes the significant fields shown in the display.

Table 2 *debug ip nat h323 Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature.
H.225 and H.245:	Protocol of the packet.
[1]	Indicates that the packet is moving from a host inside the network to one outside the network.
[0]	Indicates that the packet is moving from a host outside the network to one inside the network.

The following is sample output from the **debug ip nat sip** command. In this example, one IP phone registers with a Cisco SIP proxy and then calls another IP phone. The debug output displays the SIP messages that NAT recognizes and the embedded IP addresses contained in those messages.

```
Router# debug ip nat sip
NAT:SIP:[0] processing REGISTER message
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] message body found
NAT:SIP:[0] found address/port in SDP body:192.168.122.20
20332
NAT:SIP:[1] processing SIP/2.0 100 Trying reply message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing SIP/2.0 200 OK reply message
NAT:SIP:[1] translated embedded address
```

```

2.2.2.2->192.168.122.3
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing INVITE message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] message body found
NAT:SIP:[1] found address/port in SDP body:192.168.22.20

```

Table 3 describes the significant fields shown in the display.

Table 3 *debug ip nat sip Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature.
SIP:	Protocol of the packet.
[1]	Indicates that the packet is moving from a host inside the network to one outside the network.
[0]	Indicates that the packet is moving from a host outside the network to one inside the network.

The following is sample output from the **debug ip nat vrf** command.

```

Router# debug ip nat vrf
6d00h:NAT:address not stolen for 192.168.121.113, proto 1 port 7224
6d00h:NAT:creating portlist proto 1 globaladdr 2.2.2.10
6d00h:NAT:Allocated Port for 192.168.121.113 -> 2.2.2.10:wanted 7224 got 7224
6d00h:NAT:i:icmp (192.168.121.113, 7224) -> (168.58.88.2, 7224) [2460]
6d00h:NAT:s=192.168.121.113->2.2.2.10, d=168.58.88.2 [2460] vrf=> shop

6d00h:NAT*:o:icmp (168.58.88.2, 7224) -> (2.2.2.10, 7224) [2460] vrf=> shop
6d00h:NAT*:s=168.58.88.2, d=2.2.2.10->192.168.121.113 [2460] vrf=> shop

6d00h:NAT:Allocated Port for 192.168.121.113 -> 2.2.2.10:wanted 7225 got 7225
6d00h:NAT:i:icmp (192.168.121.113, 7225) -> (168.58.88.2, 7225) [2461]
6d00h:NAT:s=192.168.121.113->2.2.2.10, d=168.58.88.2 [2461] vrf=> shop
6d00h:NAT*:o:icmp (168.58.88.2, 7225) -> (2.2.2.10, 7225) [2461] vrf=> shop
6d00h:NAT*:s=168.58.88.2, d=2.2.2.10->192.168.121.113 [2461] vrf=> shop
6d00h:NAT:Allocated Port for 192.168.121.113 -> 2.2.2.10:wanted 7226 got 7226
6d00h:NAT:i:icmp (192.168.121.113, 7226) -> (168.58.88.2, 7226) [2462]
6d00h:NAT:s=192.168.121.113->2.2.2.10, d=168.58.88.2 [2462] vrf=> shop

```

Table 4 describes the significant fields shown in the display.

Table 4 *debug ip nat vrf Field Descriptions*

Field	Description
vrf=>	Indicates NAT is applied to a particular VPN.

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

```
ip nat inside source {list {access-list-number | access-list-name} | route-map name} {interface
type number | pool pool-name} vrf vrf-name [overload]
```

```
no ip nat inside source {list {access-list-number | access-list-name} | route-map name}
{interface type number | pool pool-name} vrf vrf-name [overload]
```

Static NAT

```
ip nat inside source {static {local-ip global-ip} vrf vrf-name [extendable] [no-alias]
[no-payload] [route-map] [redundancy group-name]}
```

```
no ip nat inside source {static {local-ip global-ip} vrf vrf-name [extendable] [no-alias]
[no-payload] [route-map] [redundancy group-name]}
```

Port Static NAT

```
ip nat inside source {static {tcp | udp local-ip local-port global-ip global-port} [extendable]
[no-alias] [no-payload]}
```

```
no ip nat inside source {static {tcp | udp local-ip local-port global-ip global-port} [extendable]
[no-alias] [no-payload]}
```

Network Static NAT

```
ip nat inside source {static {network local-network global-network mask} [extendable]
[no-alias] [no-payload]}
```

```
no ip nat inside source {static {network local-network global-network mask} [extendable]
[no-alias] [no-payload]}
```

Syntax Description

list <i>access-list-number</i>	Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
route-map <i>name</i>	Specifies the named route-map.
interface <i>type</i>	Specifies the interface type for the global address.
interface <i>number</i>	Specifies the interface number for the global address.
pool <i>pool-name</i>	Specifies the pool from which global IP addresses are allocated dynamically.
vrf <i>vrf-name</i>	Associates the NAT translation rule with a particular VPN routing/forwarding (VRF) instance.

overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
static <i>local-ip</i>	Sets up a single static translation. The argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
<i>local-port</i>	Sets the local TCP/UDP port in a range from 1-65535.
static <i>global-ip</i>	Sets up a single static translation. The argument establishes the globally unique IP address of an inside host as it appears to the outside world.
<i>global-port</i>	Sets the global TCP/UDP port in a range from 1-65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits an alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy <i>group-name</i>	(Optional) Establishes NAT redundancy.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network <i>local-network</i>	Specifies the local subnet translation.
<i>global-network</i>	Specifies the global subnet translation.
<i>mask</i>	Establishes the IP Network mask to be with subnet translations.

Defaults

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use route maps with static translations, and the route-map <i>name</i> keyword and argument combination was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the redundancy <i>redundancy-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the no-payload keyword was added.
12.2(13)T	The vrf keyword and the <i>vrf-name</i> argument were added.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the router through the inside interface and packets sourced from the router are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or the 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following examples translate only traffic local to the providers edge device running NAT (NAT-PE).

```
ip nat inside source list 1 interface e0 pool mypool vrf shop overload
ip nat inside source list 1 interface e0 pool mypool vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 192.1.1.1
ip route vrf bank 0.0.0.0 0.0.0.0 192.1.1.1
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
!
ip nat inside source list 1 interface e1 pool mypool vrf shop overload
ip nat inside source list 1 interface e1 pool mypool vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 172.1.1.1 global
ip route vrf bank 0.0.0.0 0.0.0.0 172.1.1.1 global
access-list 1 permit 10.1.1.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

```
ip nat outside source {list {access-list-number | access-list-name} | route-map name} pool
pool-name vrf vrf-name [add-route]
```

```
no ip nat outside source {list {access-list-number | access-list-name} | route-map name} pool
pool-name vrf vrf-name [add-route]
```

Static NAT

```
ip nat outside source static {global-ip local-ip} vrf vrf-name [add-route] [extendable] [no-alias]
[no-payload] [redundancy group-name]
```

```
no ip nat outside source static {global-ip local-ip} vrf vrf-name [add-route] [extendable]
[no-alias] [no-payload] [redundancy group-name]
```

Port Static NAT

```
ip nat outside source static {tcp | udp global-ip global-port local-ip local-port} [add-route]
[extendable] [no-alias] [no-payload]
```

```
no ip nat outside source static {tcp | udp global-ip global-port local-ip local-port} [add-route]
[extendable] [no-alias] [no-payload]
```

Network Static NAT

```
ip nat outside source static network global-network local-network mask [add-route]
[extendable] [no-alias] [no-payload]
```

```
no ip nat outside source static network global-network local-network mask [add-route]
[extendable] [no-alias] [no-payload]
```

Syntax Description

list <i>access-list-number</i>	Standard IP access list number. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
route-map <i>name</i>	Specifies a named route map.
pool <i>pool-name</i>	Specifies the name of the pool from which global IP addresses are allocated.
add-route	(Optional) Adds a static route for the outside local address.
static <i>global-ip</i>	Sets up a single static translation. The argument establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space.

static <i>local-ip</i>	Sets up a single static translation. The argument establishes the local IP address of an outside host as it appears to the inside world. The address was allocated from address space routable on the inside (RFC 1918, <i>Address Allocation for Private Internets</i>).
vrf <i>vrf-name</i>	Associates the NAT translation rule with a particular VRF.
extendable	(Optional) Extends the transmission.
no-alias	(Optional) Prohibits an alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of embedded address or port in the payload.
redundancy <i>group-name</i>	(Optional) Enables the NAT redundancy operation.
tcp	Transmission Control Protocol
udp	User Datagram Protocol

Defaults

No translation of source addresses coming from the outside to the inside network occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the redundancy <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the no-payload keyword was added.
12.2(13)T	The keyword vrf and the argument <i>vrf-name</i> were added.

Usage Guidelines

You might have IP addresses that are not legal, officially assigned IP addresses. Perhaps you chose IP addresses that officially belong to another network. The case of an address used illegally and legally is called *overlapping*. You can use NAT to translate inside addresses that overlap with outside addresses. Use this feature if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or routers.

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

Examples

The following example translates between inside hosts addressed from the 9.114.11.0 network to the globally unique 171.69.233.208/28 network. Further packets from outside hosts addressed from the 9.114.11.0 network (the true 9.114.11.0 network) are translated to appear to be from the 10.0.1.0/24 network.

```

ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 9.114.11.39 255.255.255.0
 ip nat inside
access-list 1 permit 9.114.11.0 0.0.0.255

```

The following example shows NAT configured on the PE with a static route to the shared service for the gold and silver VPNs. NAT is configured as inside source static 1 to 1 translations.

```

ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 168.58.18.0 0.0.0.255
ip nat inside source static 192.168.121.33 2.2.2.1 vrf gold
ip nat inside source static 192.169.121.33 2.2.2.2 vrf silver

```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** command in EXEC mode.

show ip nat translations [**verbose**] [**vrf vrf-name**]

Syntax Description	Parameter	Description
	verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
	vrf vrf-name	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(13)T	The vrf keyword and <i>vrf-name</i> argument were added.

Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Router# show ip nat translations

Pro Inside global      Inside local      Outside local      Outside global
--- 171.69.233.209     192.168.1.95     ---                ---
--- 171.69.233.210     192.168.1.89     ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Router# show ip nat translations

Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ip nat translations verbose

Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
      create 00:00:02, use 00:00:00, flags: extended
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
      create 00:01:13, use 00:00:50, flags: extended
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
      create 00:00:02, use 00:00:00, flags: extended
```

The following is sample output that includes the **vrf** keyword:

```

Router# Show ip nat translations vrf
Pro Inside global      Inside local      Outside local     Outside global
--- 2.2.2.1            192.168.121.113  ---              ---
--- 2.2.2.2            192.168.122.49  ---              ---
--- 2.2.2.11           192.168.11.1    ---              ---
--- 2.2.2.12           192.168.11.3    ---              ---
--- 2.2.2.13           140.48.5.20     ---              ---

Pro Inside global      Inside local      Outside local     Outside global
--- 2.2.2.3            192.168.121.113  ---              ---
--- 2.2.2.4            192.168.22.49   ---              ---

```

Table 5 describes the significant fields shown in the display.

Table 5 show ip nat translations Field Descriptions

Field	Description
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: <ul style="list-style-type: none"> extended—Extended translation static—Static translation destination—Rotary translation outside—Outside translation timing out—Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.

Command	Description
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.

Glossary

CE—customer edge. Customer’s edge device connecting to an MPLS cloud.

MPLS—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

NAT—Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

NAT-PE—Provider edge device running NAT.

PE—provider edge. Provider edge device on an MPLS cloud.

VPN—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VRF—A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

**Note**

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