Integrating NAT with MPLS VPNs

Last Updated: November 29, 2012

The 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

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.

- 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

This feature was introduced in Cisco IOS XE 2.5. For a list of restrictions, see the Cisco IOS XE 2 Release Notes .

Information About Integrating NAT with MPLS VPNs

Benefits of NAT Integration with MPLS VPNs

For MPLS service providers to provide value-added services such as Internet connectivity, domain name servers (DNS), and VoIP service to their customers, their customers’ IP addresses be unique 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 can be implemented on the PE router in the following scenarios:

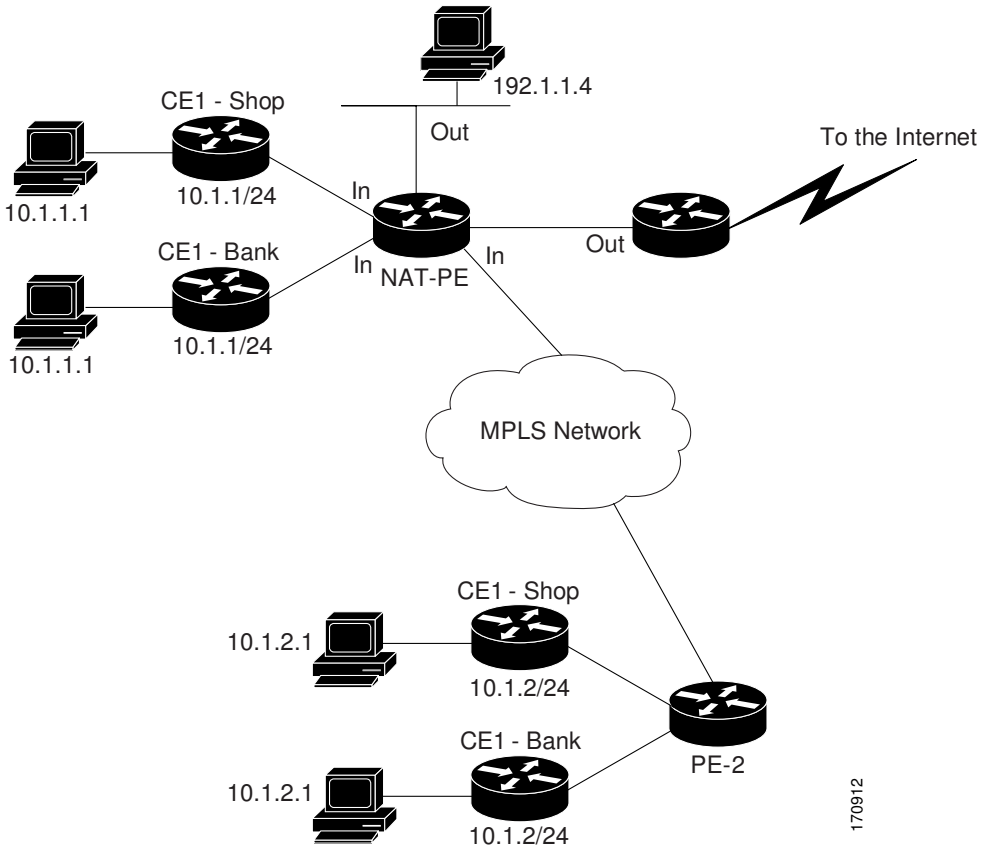
- Service point--Shared access can be from a generic interface or from a VPN interface.
- NAT point--NAT can be configured on the PE router that is directly connected to the shared access gateway, or on the PE router that is not directly connected to the shared access gateway.
- NAT interface--The shared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

The figure below shows a typical NAT integration with MPLS VPNs. The PE router is 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 want to configure for your network:

- Configuring Inside Dynamic NAT with MPLS VPNs, page 3
- Configuring Inside Static NAT with MPLS VPNs, page 5
- Configuring Outside Dynamic NAT with MPLS VPNs, page 7
- Configuring Outside Static NAT with MPLS VPNs, page 8

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 each VPN being configured
6. **ip route vrf** *vrf-name prefix mask interface-type interface-number next-hop-address*
7. Repeat Step 6 for each VPN 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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* **Example:** `Router(config)# ip nat pool inside 10.2.2.10 10.2.2.10 netmask 255.0.0.0`	Defines a pool of IP addresses for NAT.
Step 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**] **Example:** `Router(config)# ip nat inside source list 1 pool mypool vrf shop overload`	Allows NAT to be configured on a particular VPN. • For a list of restrictions, see the Cisco IOS XE 2 Release Notes .
Step 5	Repeat Step 4 for each VPN being configured	Allows NAT to be configured on additional VPNs.

	Command or Action	Purpose
Step 6	**ip route vrf** *vrf-name prefix mask interface-type interface-number next-hop-address* **Example:** `Router(config)# ip route vrf shop 0.0.0.0 0.0.0.0 fastethernet 0 192.168.88.2`	Allows the route to be shared by customers using the specified VPN.
Step 7	Repeat Step 6 for each VPN being configured.	Allows the route to be shared by customers using additional specified VPNs.
Step 8	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 9	**show ip nat translations vrf** *vrf-name* **Example:** `Router# show ip nat translations vrf shop`	(Optional) Displays the settings used by 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. • 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 10.2.2.1 vrf shop`
		Enables inside static translation on the specified VRF.
		• For a list of restrictions, see the Cisco IOS XE 2 Release Notes .

Step 4	Repeat Step 3 for each VPN being configured.	Enables inside static translation on additional VRFs.

Step 5	**ip route vrf** *vrf-name* **prefix** *prefix mask next-hop-address* **global**
	
	Example:
	`Router(config)#`
	`ip route vrf shop prefix 0.0.0.0 0.0.0.0 192.168.88.2 global`
		Allows the route to be shared by customers using the specified VPN.

Step 6	Repeat Step 5 for each VPN being configured.	Allows the route to be shared by customers using additional specified VPNs.
Step 7	**exit** **Example:** `Router config)# exit`	Returns to privileged EXEC mode.

	Command or Action	Purpose
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** *name 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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**ip nat pool** *name global-ip local-ip* **netmask** *netmask*
	
	Example:
	
	`Router(config)#`
	`ip nat pool out_pool 10.4.4.1 10.4.4.254 netmask 255.0.0.00`
		Allows the configured VRF to be associated with the NAT translation rule.

	Command or Action	Purpose
Step 4	**ip nat inside source static** *local-ip global-ip* **vrf** *vrf-name* **Example:** `Router(config)# ip nat inside source static 192.168.121.113 10.2.2.1 vrf shop`	Allows the route to be shared by customers using the specified VPN. • For a list of restrictions, see the Cisco IOS XE 2 Release Notes .
Step 5	Repeat Step 4 for each VRF being configured.	Allows the route to be shared by customers using additional specified VPNs.
Step 6	**ip nat outside source static** *global-ip local-ip* **vrf** *vrf-name* **Example:** `Router(config)# i p nat outside source static 192.168.88.2 10.4.4.1 vrf shop`	Enables NAT translation of the outside source address.
Step 7	**exit** **Example:** `Router(config)# 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 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** | **memory** | **network**}
3. **ip nat pool** *name 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** *name global-ip local-ip* **netmask** *netmask*
	
	Example:
	`Router(config)# i`
	`p nat pool in_pool 10.2.1.1 10.2.1.254 netmask`
	`255.0.0.0`
		Allows the configured VRF to be associated with a NAT translation rule.

Step 4	Repeat Step 3 for each pool being configured.	Allows the configured VRF to be associated with additional NAT translation rules.

Step 5	**ip nat inside source list** *access-list-number* **pool** *pool-name* **vrf** *vrf-name*
	
	Example:
	`Router(config)#`
	`ip nat inside source list 1 pool in_pool vrf shop`
		Allows the route to be shared by several customers.
		• For a list of restrictions, see the Cisco IOS XE 2 Release Notes .

	Command or Action	Purpose
Step 6	Repeat Step 5 for each pool being configured.	Defines the access list.

Step 7	**ip nat outside source static** *global-ip local-ip* **vrf** *vrf-name*
	
	Example:
	
	`Router(config)#`
	`ip nat outside source static 192.168.88.2 10.4.4.1 vrf shop`
		Allows the route to be shared by customers using the specified VPN.

Step 8	Repeat Step 7 for all VPNs being configured.	Allows the route to be shared by customers using additional specified VPNs.
Step 9	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 10	**show ip nat translations vrf** *vrf-name* **Example:** `Router# show ip nat translations vrf shop`	(Optional) Displays the settings used by VRF translations.

Configuration Examples for Integrating NAT with MPLS VPNs

Configuring Inside Dynamic NAT with MPLS VPNs Example

The following example shows how to configure inside Dynamic NAT with MPLS VPNs:

```
!
ip nat pool inside 10.2.2.10 10.2.2.10 netmask 255.0.0.0
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 fastethernet1/3 192.168.88.2
ip route vrf bank 0.0.0.0 0.0.0.0 fastethernet1/3 192.168.88.2
ip route vrf park 0.0.0.0 0.0.0.0 fastethernet1/3 192.168.88.2
!
access-list 1 permit 192.168.0.0 0.0.255.255
```

Configuring Inside Static NAT with MPLS VPNs Example

The following example shows how to configure inside static NAT with MPLS VPNs:

```
!
ip nat inside source static 192.168.121.113 10.2.2.1 vrf shop
ip nat inside source static 192.168.122.49 10.2.2.2 vrf shop
ip nat inside source static 192.168.121.113 10.2.2.3 vrf bank
ip nat inside source static 192.168.22.49 10.2.2.4 vrf bank
ip nat inside source static 192.168.121.113 10.2.2.5 vrf park
ip nat inside source static 192.168.22.49 10.2.2.6 vrf park
ip nat inside source static 192.168.11.1 10.2.2.11 vrf shop
ip nat inside source static 192.168.11.3 10.2.2.12 vrf shop
ip nat inside source static 140.48.5.20 10.2.2.13 vrf shop
!
ip route 10.2.2.1 255.255.255.255 fastethernet1/0 192.168.121.113
ip route 10.2.2.2 255.255.255.255 fastethernet1/0 192.168.121.113
ip route 10.2.2.3 255.255.255.255 Serial2/1.1 192.168.121.113
ip route 10.2.2.4 255.255.255.255 Serial2/1.1 192.168.121.113
ip route 10.2.2.5 255.255.255.255 fastethernet0/0 192.168.121.113
ip route 10.2.2.6 255.255.255.255 fastethernet0/0 192.168.121.113
ip route 10.2.2.11 255.255.255.255 fastethernet1/0 192.168.121.113
ip route 10.2.2.12 255.255.255.255 fastethernet1/0 192.168.121.113
ip route 10.2.2.13 255.255.255.255 fastethernet1/0 192.168.121.113
```

Configuring Outside Dynamic NAT with MPLS VPNs Example

The following example shows how to configure outside dynamic NAT with MPLS VPNs:

```
!
ip nat pool outside 10.4.4.1 10.4.4.254 netmask 255.0.0.0
ip nat inside source static 192.168.121.113 10.2.2.1 vrf shop
ip nat inside source static 192.168.122.49 10.2.2.2 vrf shop
ip nat inside source static 192.168.121.113 10.2.2.3 vrf bank
ip nat inside source static 192.168.22.49 10.2.2.4 vrf bank
ip nat inside source static 192.168.121.113 10.2.2.5 vrf park
ip nat inside source static 192.168.22.49 10.2.2.6 vrf park
ip nat outside source list 1 pool outside
!
```

Configuring Outside Static NAT with MPLS VPNs Example

The following example shows how to configure outside static NAT with MPLS VPNs:

```
!
ip default-gateway 10.1.15.1
ip nat pool inside1 10.2.1.1 10.2.1.254 netmask 255.0.0.0
ip nat pool inside2 10.2.2.1 10.2.2.254 netmask 255.0.0.0
ip nat pool inside3 10.2.3.1 10.2.3.254 netmask 255.0.0.0
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 192.168.88.2 10.4.4.1 vrf bank
ip nat outside source static 10.68.58.1 10.4.4.2 vrf park
ip nat outside source static 192.168.88.1 10.4.4.3 vrf shop
ip classless
ip route 172.16.10.0 255.255.255.0 fastethernet 1/0 192.168.121.113
ip route 172.16.11.0 255.255.255.0 Serial 2/1.1 192.168.121.113
ip route 172.16.12.0 255.255.255.0 fastethernet 0/0 192.168.121.113
ip route vrf shop 0.0.0.0 0.0.0.0 192.168.88.2 global
ip route vrf bank 0.0.0.0 0.0.0.0 192.168.88.2 global
ip route vrf park 0.0.0.0 0.0.0.0 192.168.88.2 global
no ip http server
!
access-list 1 permit 192.168.0.0 0.0.255.255
```

Where to Go Next

For more information about configuring IP applications and services, see the *IP SLAs Configuration Guide Cisco IOS XE Release 3S*.

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*
Configuring an access list	IP Access List Sequence Numbering
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
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

Technical Assistance

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

Feature Information for Integrating NAT with MPLS VPNs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Integrating NAT with MPLS VPNs

Feature Name	Releases	Feature Configuration Information
NAT Integration with MPLS VPNs feature	Cisco IOS XE Release 2.5	This feature allows multiple Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) to be configured on a single device to work together.

1 **Not all supported RFCs are listed.**