Performance Routing with NAT

Performance Routing (PfR) introduced support for the control of traffic class routing using static routing in networks using NAT with the introduction of a new keyword to an existing NAT command. When PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons.

When the new keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface for which the NAT translation was created.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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.

Restrictions for Performance Routing with NAT

On Cisco Catalyst 6500 Switch platforms a flow mask conflict has been seen when NAT is configured in a PfR-managed network. Conflicting flow mask requirements can cause traffic to be switched in software. To resolve this conflict, add the following NAT configuration:

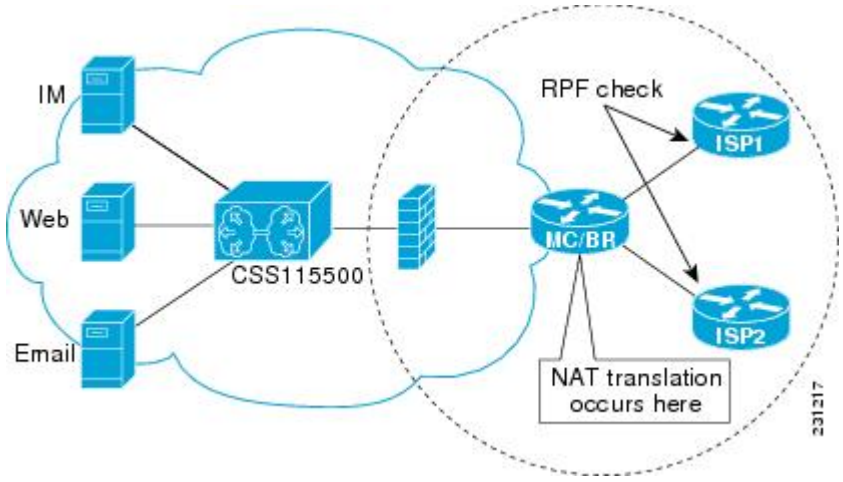
```
mls ip nat netflow-frag-l4-zero
```

Information About Performance Routing with NAT

PfR and NAT

When Cisco IOS PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons. Packets are dropped at the ingress router performing Unicast RPF because PfR changes the route for an outgoing packet for a traffic class from one exit interface to another after the NAT translation from a private IP address to a public IP address is performed. When the packet is transmitted, Unicast RPF filtering at the ingress router (for example, an ISP router) will show a different source IP address from the source IP address pool assigned by NAT, and the packet is dropped. For example, the figure below shows how PfR works with NAT.

Figure 1: PfR with NAT



The NAT translation occurs at the router that is connected to the internal network, and this router can be a border router or a combined master controller and border router. If PfR changes routes to optimize traffic class performance and to perform load balancing, traffic from the border router in the figure above that was routed through the interface to ISP1 may be rerouted through the interface to ISP2 after the traffic performance is measured and policy thresholds are applied. The RPF check occurs at the ISP routers and any packets that

are now routed through ISP2 will fail the RPF check at the ingress router for ISP2 because the IP address of the source interface has changed.

The solution involves a minimal configuration change with a new keyword, **oer**, that has been added to the**ip nat inside source** command. When the**oer** keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface for which the NAT translation was created. For example, PfR is configured to manage traffic on a border router with two interfaces, InterfaceA to ISP1 and InterfaceB to ISP2 in the figure above. PfR is first configured to control a traffic class representing Web traffic and the NAT translation for this traffic already exists with the source IP address in the packets set to InterfaceA. PfR measures the traffic performance and determines that InterfaceB is currently the best exit for traffic flows, but PfR does not change the existing flow. When PfR is then configured to learn and measure a traffic class representing e-mail traffic, and the e-mail traffic starts, the NAT translation is done for InterfaceB. The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported. Network configurations using NAT and devices such as PIX firewalls that do not run Cisco IOS software are not supported.

Network Address Translation (NAT)

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) address in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise only one address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind that one address.

NAT is also used at the Enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

For more details about NAT, see the “Configuring NAT for IP Address Conservation” chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

Inside Global Addresses Overloading

You can conserve addresses in the inside global address pool by allowing the router to use one global address for many local addresses. When this overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses.

How to Configure Performance Routing with NAT

Configuring PfR to Control Traffic with Static Routing in Networks Using NAT

Perform this task to allow PfR to control traffic with static routing in a network using NAT. This task allows PfR to optimize traffic classes while permitting your internal users access to the internet.

When Cisco IOS PfR and NAT functionality are configured on the same router and PfR controls the routing for a traffic class using static routing, some applications may fail to operate due to dropped packets. This

dropping of packets behavior is seen when static routing is used to connect to multiple ISPs from the same router, PfR uses static routing to control the traffic class routing, and one or more of the ISPs use Unicast Reverse Path Forwarding (Unicast RPF) filtering for security reasons.

In this task, the **pfr** keyword is used with the**ip nat inside source** command. When the**pfr** keyword is configured, new NAT translations are given the source IP address of the interface that PfR has selected for the packet and PfR forces existing flows to be routed through the interface where the NAT translation was created. This task uses a single IP address but an IP address pool can also be configured. For a configuration example using an IP address pool, see "Configuring PfR to Control Traffic with Static Routing in Networks Using NAT" section.

Note The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported.

For more details about configuring NAT, see the "Configuring NAT for IP Address Conservation" chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *ip-address*mask
4. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
5. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
6. **match interface** *interface-type interface-number* [*...interface-type interface-number*]
7. **exit**
8. Repeat Step 4 through Step 7 for more route map configurations, as required.
9. **ip nat inside source** {**list** {*access-list-number*| *access-list-name*} | **route-map** *map-name*} {**interface** *type number*| **pool** *name*} [**mapping-id** *map-id* | **overload**| **reversible**| **vrf** *vrf-name*][**pfr**]
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat inside**
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask*
16. **ip nat outside**
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**permit** | **deny**} *ip-address*mask **Example:** `Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255`	Defines a standard access list permitting the IP addresses that are to be translated. • The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access list.) An access list that is too permissive can lead to unpredictable results.
Step 4	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map isp-1 permit 10`	Enters route-map configuration mode to configure a route map. • The example creates a route map named BGP.
Step 5	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} **Example:** `Router(config-route-map)# match ip address access-list 1`	Creates an access list or prefix list match clause entry in a route map to identify traffic to be translated by NAT. • The example references the access list created in Step 3 that specifies the 10.1.0.0 0.0.255.255. prefix as match criteria.
Step 6	**match interface** *interface-type interface-number* [*...interface-type interface-number*] **Example:** `Router(config-route-map)# match interface serial 1/0`	Creates a match clause in a route map to distribute any routes that match out one of the interfaces specified. • The example creates a match clause to distribute routes that pass the match clause in Step 5 through serial interface 1/0.
Step 7	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.
Step 8	Repeat Step 4 through Step 7 for more route map configurations, as required.	--

	Command or Action	Purpose
Step 9	**ip nat inside source** {**list** {*access-list-number*| *access-list-name*} | **route-map** *map-name*} {**interface** *type number*| **pool** *name*} [**mapping-id** *map-id* | **overload**| **reversible**| **vrf** *vrf-name*][**pfr**] **Example:** `Router(config)# ip nat inside source interface FastEthernet1/0 overload pfr`	Establishes dynamic source translation with overloading, specifying the interface. • Use the **interface** keyword and type and number arguments to specify an interface. • Use the **pfr** keyword to allow PfR to operate with NAT and control traffic class routing using static routing.
Step 10	**interface** *type number* **Example:** `Router(config)# interface FastEthernet1/0`	Specifies an interface and enters interface configuration mode.
Step 11	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.114.11.8 255.255.255.0`	Sets a primary IP address for the interface.
Step 12	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Marks the interface as connected to the inside.
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to configuration mode.
Step 14	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Specifies a different interface and returns to interface configuration mode.
Step 15	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.17.233.208 255.255.255.0`	Sets a primary IP address for the interface.
Step 16	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Marks the interface as connected to the outside.

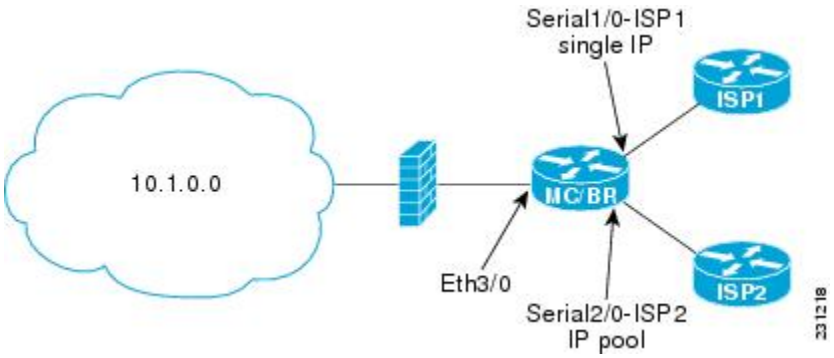
	Command or Action	Purpose
Step 17	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Performance Routing with NAT

Example Configuring PfR to Control Traffic with Static Routing in Networks Using NAT

The following configuration example configures a master controller to allow PfR to control traffic with static routing in a network using NAT. This example shows how to use a pool of IP addresses for the NAT translation.

Figure 2: PfR and NAT Network Diagram



In the figure above there is a combined master controller and border router that is connected to the Internet through two different ISPs. The configuration below allows PfR to optimize traffic classes while permitting the internal users access to the internet. In this example the traffic classes to be translated using NAT are specified using an access list and a route map. The use of a pool of IP addresses for NAT translation is then configured and the **pfr** keyword is added to the **ip nat inside source** command to configure PfR to keep existing traffic classes flowing through the interface that is the source address that was translated by NAT. New NAT translations can be given the IP address of the interface that PfR has selected for the packet.

Note The PfR static routing NAT solution is a single box solution and configurations with interfaces on multiple routers using NAT and managed by PfR are not supported.

```
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# route-map isp-2 permit 10BGP permit 10
```

```
Router(config-route-map)# match ip address access-list 1
Router(config-route-map)# match interface serial 2/0
Router(config-route-map)# exit
Router(config)# ip nat pool ISP2 209.165.201.1 209.165.201.30 prefix-length 27
Router(config)# ip nat inside source route-map isp-2 pool ISP2 pfr
Router(config)# interface FastEthernet 3/0
Router(config-if)# ip address 10.1.11.8 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface serial 1/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface serial 2/0
Router(config-if)# ip address 172.17.233.208 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# end
```

Where to Go Next

For information about other Performance Routing features or general conceptual material, see the documents in the “Related Documents” section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	“Configuring Basic Performance Routing” module
Advanced PfR configuration	“Configuring Advanced Performance Routing” module
Concepts required to understand the Performance Routing operational phases	“Understanding Performance Routing” module
General information about NAT	“Configuring NAT for IP Address Conservation” module
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

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/cisco/web/support/index.html

Feature Information for Performance Routing with NAT

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 Performance Routing with NAT

Feature Name	Releases	Feature Information
Support for NAT and Static Routing[1]	12.3(14)T 12.2(33)SRB	Support to allow PfR to control traffic class routing using static routing in networks using NAT. The following command was modified by this feature: **ip nat inside source**.

1 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.