IP Multicast Dynamic NAT

The IP Multicast Dynamic Network Address Translation (NAT) feature supports the source address translation of multicast packets. You can use source address translation when you want to connect to the Internet, but not all your hosts have globally unique IP addresses. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network. The IP multicast dynamic translation establishes a one-to-one mapping between an inside local address and one of the addresses from the pool of outside global addresses.

Restrictions for IP Multicast Dynamic NAT

The IP Multicast Dynamic NAT feature does not support:

- IPv4-to-IPv6 address translation.
- Multicast destination address translation.
- Port Address Translation (PAT) overloading for multicast.
- Source and destination address translation.
- Unicast-to-multicast address translation.

Note To configure multicast ACL for a NAT inside interface, ensure that you configure the ACL to allow IP addresses before and after NAT translation. If you do not configure the ACL to permit IP addresses after NAT translation, the MFIB table does not contain (S,G) entry and this can cause issues in certain deployments.

Information About IP Multicast Dynamic NAT

How NAT Works

A device that is configured with NAT has at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit device between a stub domain and the backbone. When a packet exits the domain, NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. If NAT cannot allocate an address because it has run out of addresses, it drops the packet. Then, NAT sends an Internet Control Message Protocol (ICMP) host unreachable packet to the destination.

Uses of NAT

NAT can be used for the following applications:

- When you want to connect to the Internet, but not all of your hosts have globally unique IP addresses. NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT is configured on the router at the border of a stub domain (referred to as the *inside network*) and a public network such as the Internet (referred to as the *outside network*). NAT translates internal local addresses to globally unique IP addresses before sending packets to the outside network. As a solution to the connectivity problem, NAT is practical only when relatively few hosts in a stub domain communicate outside of the domain at the same time. When this is the case, only a small subset of the IP addresses in the domain must be translated into globally unique IP addresses when outside communication is necessary, and these addresses can be reused when they are no longer in use.
- When you must change your internal addresses. Instead of changing the internal addresses, which can be a considerable amount of work, you can translate them by using NAT.
- When you want to do basic load sharing of TCP traffic. You can map a single global IP address to many local IP addresses by using the TCP load distribution feature.

NAT Inside and Outside Addresses

The term *inside* in a Network Address Translation (NAT) context refers to networks owned by an organization that must be translated. When NAT is configured, hosts within this network have addresses in one space (known as the *local* address space). These hosts appear to those users outside the network as being in another space (known as the *global* address space).

Similarly, the term *outside* refers to those networks to which the stub network connects, and which are not under the control of an organization. Also, hosts in outside networks can be subject to translation, and can thus have local and global addresses. NAT uses the following definitions:

- Inside local address—An IP address that is assigned to a host on the inside network. The address that the Network Information Center (NIC) or service provider assigns is probably not a legitimate IP address.
- Inside global address—A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.

- Outside local address—The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from the address space that is routable on the inside.
- Outside global address—The IP address that is assigned to a host on the outside network by the owner of the host. The address is allocated from a globally routable address or network space.

NAT supports the following VRFs:

Table 1: VRF NAT Support

NAT Inside Interface	NAT Outside Interface	Condition
Global VRF (also referred to as a non-VRF interface)	Global VRF (also referred to as a non-VRF interface)	Normal
VRF X	Global VRF (also referred to as a non-VRF interface)	When NAT is not configured for Match-in-VRF support. For more details, see the *Match-in-VRF Support for NAT* chapter.
VRF X	VRF X	When both inside and outside interfaces are in the same VRF, and NAT is configured with Match-in-VRF support.

This section describes the following topics:

- Inside Source Address Translation
- Overloading of Inside Global Addresses

Dynamic Translation of Addresses

Dynamic translation establishes a mapping between an inside local address and a pool of global addresses. Dynamic translation is useful when multiple users on a private network access the Internet. The dynamically configured pool IP address may be used as needed. It is released for use by other users when access to the Internet is no longer required.

Note When inside global or outside local addresses belong to a directly connected subnet on a NAT router, the router adds IP aliases for them. This action enables answer Address Resolution Protocol (ARP) requests. However, a situation can arise where the router itself answers packets that are not destined for it, possibly causing a security issue. This security issue can happen when an incoming Internet Control Message Protocol (ICMP) or UDP packet that is destined for one of the aliased addresses does not have a corresponding NAT translation in the NAT table. The router itself runs a corresponding service, for example, the Network Time Protocol (NTP). Such a situation might cause minor security risks.

How to Configure IP Multicast Dynamic NAT

Configuring IP Multicast Dynamic NAT

Note IP multicast dynamic translation establishes a one-to-one mapping between an inside local address and one of the addresses from the pool of outside global addresses

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**type** {**match-host** | **rotary**}]
4. **access-list** *access-list-number* **permit** *source-address wildcard-bits* [**any**]
5. **ip nat inside source list** *access-list-number* **pool** *name*
6. **ip multicast-routing distributed**
7. **interface** *type number*
8. **ip address** *ip-address mask*
9. **ip pim sparse-mode**
10. **ip nat inside**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **ip pim sparse-mode**
15. **ip nat outside**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**type** {**match-host** | **rotary**}] **Example:** `Router(config)# ip nat pool mypool 10.41.10.1 10.41.10.23 netmask 255.255.255.0`	Defines a pool of global addresses to be allocated as needed.
Step 4	**access-list** *access-list-number* **permit** *source-address wildcard-bits* [**any**] **Example:** `Router(config)# access-list 100 permit 10.3.2.0 0.0.0.255 any`	Defines a standard access list for the inside addresses that are to be translated.
Step 5	**ip nat inside source list** *access-list-number* **pool** *name* **Example:** `Router(config)# ip nat inside source list 100 pool mypool`	Establishes dynamic source translation, specifying the access list defined in the prior step.
Step 6	**ip multicast-routing distributed** **Example:** `Router(config)# ip multicast-routing distributed`	Enables Multicast Distributed Switching (MDS).
Step 7	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 8	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 9	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables sparse mode operation of Protocol Independent Multicast (PIM) on an interface.
Step 10	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Indicates that the interface is connected to the inside network (the network that is subject to NAT translation).
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 12	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/1`	Configures an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 13	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.2.2.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 14	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables sparse mode operation of PIM on an interface.
Step 15	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Indicates that the interface is connected to the outside network.
Step 16	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

Configuration Examples for IP Multicast Dynamic NAT

Example: Configuring IP Multicast Dynamic NAT

```
Router# configure terminal
Router(config)# ip nat pool mypool 10.41.10.1 10.41.10.23 netmask 255.255.255.0
Router(config)# access-list 100 permit 10.3.2.0 0.0.0.255 any
Router(config)# ip nat inside source list 100 pool mypool
Router(config)# ip multicast-routing distributed
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# ip address 10.2.2.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip nat outside
Router(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NAT commands	Cisco IOS IP Addressing Services Command Reference
Configuring NAT for IP address conservation	Configuring NAT for IP Address Conservation module

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP Multicast Dynamic NAT

Table 2: Feature Information for IP Multicast Dynamic NAT

Feature Name	Releases	Feature Information
IP Multicast Dynamic NAT	Cisco IOS XE Release 3.4S	The IP Multicast Dynamic Network Address Translation feature supports the source address translation of multicast packets. You can use source address translation when you want to connect to the Internet, but not all your hosts have globally unique IP addresses. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network. The IP multicast dynamic translation establishes a one-to-one mapping between an inside local address and one of the addresses from the pool of outside global addresses.