Network Address Translation

Network Address Translation (NAT) is a network service that translates between private and public address space. The private inside address is translated or mapped to a public routable IP address. That is required since private addresses are not routable across the internet. Conversely, all inbound traffic from the internet is translated to an original private IP address. There are a variety of NAT configuration modes available.

The primary advantage of NAT is to map multiple private IP addresses to a single or multiple public IP addresses. The ISP does not have a public IP address that is available for every private IP address. NAT allows for configuring a pool of public IP addresses. The private IP address is dynamically mapped for that internet session only. As a result there is no requirement to re-address local hosts for internet access.

The following are primary characteristics of NAT

- Conceals private IP addressing from the internet
- Easier management of internet connectivity
- Public IP address is assigned from ISP
- Translation between private and public address space

Example: NAT Address Types

Refer to the topology drawing. Identify the different NAT address types for translation.

Inside Local IP Address (192.168.1.1/24)

Private IP address assigned to a host on the inside network (RFC 1918).

Inside Global IP Address (172.33.1.1/24)

Public internet routable IP address assigned to company by an ISP.

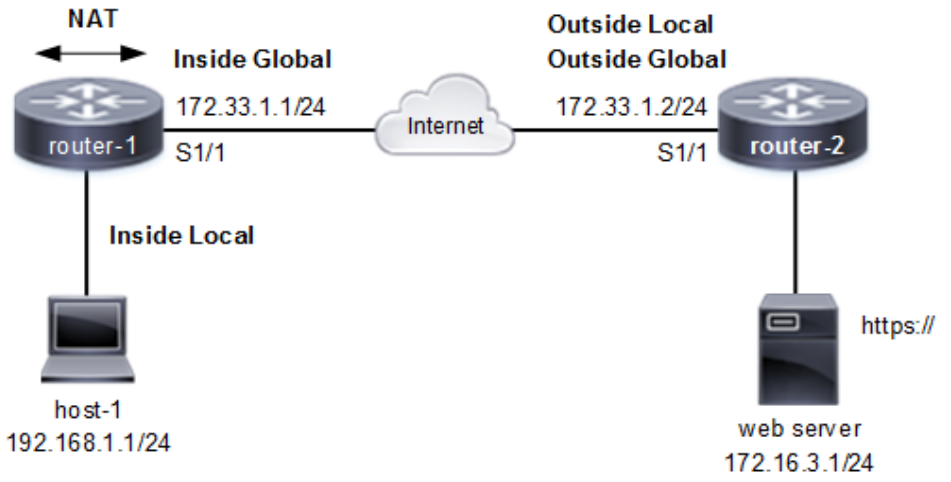
Outside Global IP Address (172.33.1.2/24)

Public internet routable IP address assigned to destination router interface.

Outside Local IP Address (172.33.1.2/24)

IP address of an outside server as it appears to the inside local network.

Figure 1 Network Address Translation



Static NAT

Static NAT translation is one-to-one (1:1) persistent mapping between local and public IP address. It is manually configured mapping of an inside local address to an outside global address. For example, three public routable IP addresses will allow three static NAT translations. There are permanent entries in the NAT translation table unless the router is turned off. They are often configured to explicitly enable a remote host connection from an outside network.

Example: Static NAT

The static NAT statement creates a 1:1 mapping between a local IP address and a global IP address. The following configures a static NAT between inside local IP address 192.168.1.1 (private) and global IP address 200.200.1.1 (internet routable).

ip nat inside source static 192.168.1.1 200.200.1.1

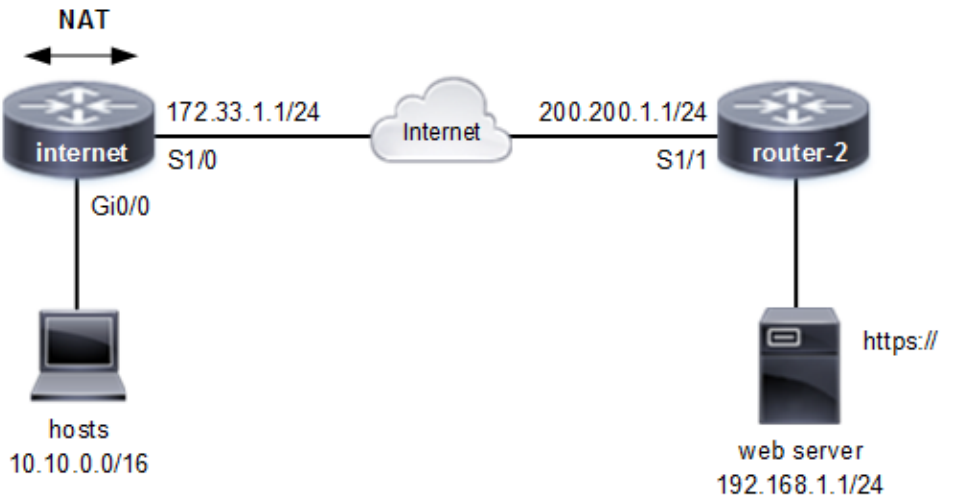
Dynamic NAT Pool

Dynamic NAT pool translates each private IP address to an available public IP address (1:1) in the NAT pool. The network administrator assigns a range of public addresses to a pool. All public IP addresses in the pool are shared by all inside private IP addresses. They are allocated for the session on a first come first served basis. The maximum number of simultaneous internet connections at any time is limited by the number of public IP addresses in the NAT pool.

Example: Dynamic NAT Pool

The following is a dynamic NAT pool configuration example. There is a NAT pool of four public IP addresses available for translation of private 10.10.0.0/16 addresses assigned to endpoint hosts.

Figure 2 Dynamic NAT



Step 1. Configure NAT inside interface on internet router.

```
interface gigabitethernet0/0
ip nat inside
exit
```

Step 2. Configure NAT outside interface on internet router.

```
interface serial1/0
ip nat outside
exit
```

Step 3. Create NAT pool **INET** and assign public range 172.33.1.2/24 to 172.33.1.5/24 on internet router.

```
ip nat pool INET 172.33.1.2 172.33.1.5 netmask 255.255.255.0
```

Step 4. Create access-list 99 on internet router to permit private hosts in address range 10.10.0.0 to 10.10.255.255 to access the internet. (wildcard mask required)

```
access-list 99 permit 10.10.0.0 0.0.255.255
```

Step 5. Assign ACL 99 to dynamic NAT pool INET .

ip nat inside source list 99 pool INET

The alternative to **netmask** keyword for NAT pool address range is **prefix-length 24** (255.255.255.0)**.** That assigns the same /24 subnet mask to all four public IP addresses.

The **source list 99** points to ACL 99 that permits a range of inside (private) IP addresses to be translated. Any private host address within the range of access list 99 have their IP address translated to a public IP address from the NAT pool. Cisco supports standard and extended access lists for NAT. The following command displays the NAT table and that translation is working correctly.

internet# **show ip nat translations**

Port Address Translation

Port Address Translation (PAT) translates private IP addresses to a single (NAT overload) public IP address. There is support for either a single public address or range of public addresses. In addition, you can also designate an outside public interface. It is the associated public address of the interface that is then used for translation.

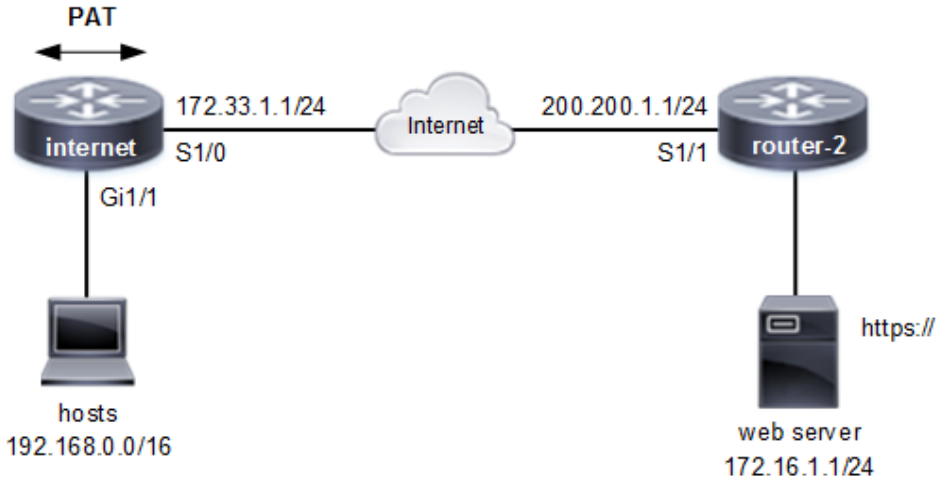
The public addressing is assigned to a NAT pool. Port address translation assigns a unique source port number to each translated private address. The host IP address for example could be identified with 200.200.1.1:**10** as the translated source IP address. The public IP address 200.200.1.1 is configured and assigned to a NAT pool. The **10** is a unique source port that is used to create a uniquely translatable IP address. There is a 16 bit source port field that enables translation of up to 65,535 private IP host addresses per public IP address. Assigning multiple public addresses to the NAT pool provide 65,535 session translations for each public address.

Inside Private		**Outside Public**
192.168.1.1:10	⟶	200.200.1.1:10
192.168.1.2:11	⟶	200.200.1.1:11
192.168.1.3:12	⟶	200.200.1.1:12

Example: Port Address Translation

The following is an example of Port Address Translation known as NAT overload. That is used to translate multiple private host addresses to a single public address.

Figure 3 Port Address Translation



Step 1. Configure NAT inside interface on internet router.

```
interface gigabitethernet1/1
ip nat inside
exit
```

Step 2. Configure NAT outside interface on internet router.

```
interface serial1/0
ip nat outside
exit
```

Step 3. Create NAT pool **cloud** and assign 172.33.1.1/24 public address.

```
ip nat pool cloud 172.33.1.1 172.33.1.1 netmask 255.255.255.0
```

Step 4. Create access-list 1 to permit private hosts in address range 192.168.0.0 to 192.168.255.255 to access the internet.

```
access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 5. Assign ACL 1 to NAT pool and enable overload feature.

```
ip nat inside source list 1 pool cloud overload
```

The **source list 1** points to ACL 1 that permits a range of inside (private) IP addresses to be translated. Any private host address within the range of access list 1 have their IP address translated to a public IP address from the NAT pool. Cisco supports standard and extended ACLs for NAT.

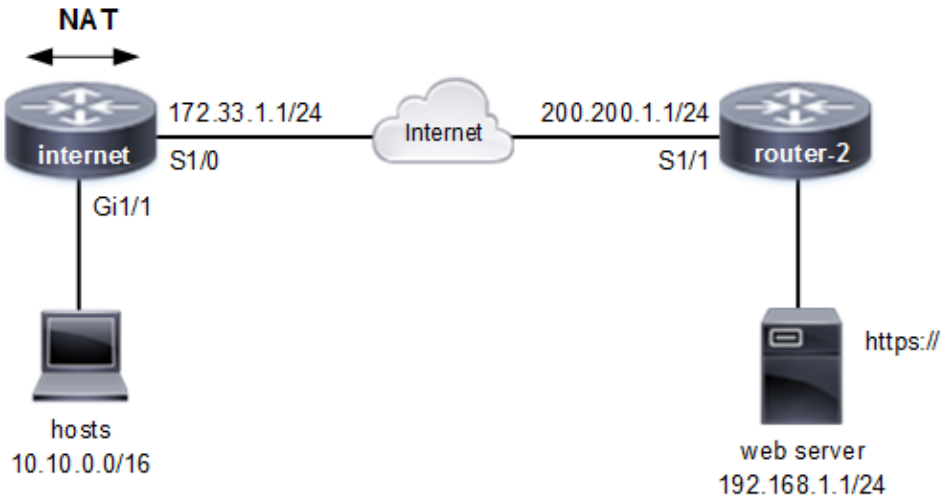
The **overload** keyword enables Port Address Translation of multiple internal IP private addresses to a single public IP address. The alternate method is to assign public interface Serial1/0 to the NAT pool. It is the same public IP address 172.33.1.1 assigned to that interface that is used for address translation.

ip nat inside source list 1 interface serial1/0 overload

Example: NAT Table

Refer to the network drawing. The network administrator recently deployed an internet router with NAT for internet connectivity. Ping from internet to router-2 verify that Layer 3 connectivity is not working. What IOS commands can verify that NAT is not the issue?

Figure 4 Network Address Translation Table



Answer

The following IOS commands are used to verify NAT operation. The results of **show running-config** list the current configuration for NAT. That would include any static or dynamic pool address translations, interfaces enabled and access control lists (ACL).

internet# **show running-config**

The following IOS command lists the translation from inside local (private) (10.10.1.1) to public (172.33.1.1) IP addressing. Network administrator can verify IP addressing is translated to the public routable IP address. There is an ACL configured to allow only a range of private IP addresses.

internet# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	172.33.1.1	10.10.1.1	---	---