NETWORK ADDRESS TRANSLATION

A GUIDE TO WHAT NETWORK ADDRESS TRANSLATION IS, WHAT IT ACCOMPLISHES, AND HOW TO CONFIGURE EACH TYPE WITHIN A NETWORK.

NAT DEFENITION AND IMPLEMENTATION

What is NAT? NAT stands for Network Address Translation. Network Address Translation is a method of remapping one IP address space into another by modifying network address information in IP datagram packet headers while in transit. The purpose of this is that IPv4 has a very limited amount of IP addresses, now that there are so many devices that can connect to a network, so it is imperative that we find a way to have devices that connect to a local network and still have them access the outside networks.

Basically it changes one IP address into another as it leaves the network. NAT is generally used in techniques today to translate a private IP address within a LAN into a public IP address that has been supplied by your ISP. NAT can also be used to translate IPv4 addresses t IPv6, however, this will not be covered here. When it comes to translating private IP addresses into public ones there are generally three separate ways in order to accomplish this: Static NAT, Dynamic NAT, and Port Address Translation (or NAT overload).

TYPES OF NETWORK ADDRESS TRANSLATION

Static NAT uses a one-to-one method of mapping public addresses and local addresses. These mappings have to be configured manually by the system administrator and need to be checked often to maintain a correct configuration. Static NAT uses one public IP and maps it directly to one local IP; as such it is only useful if there are an extremely limited number of devices. Typically this method Is used for servers that are within the local network but need to be accessed from the outside world.

Dynamic NAT uses a redefined pool of public address and assigns the users addresses on a first-come first-served basis. When a local machine needs to access the outside network it makes a request for an address, then one is assigned until it is no longer needed. If there are more users on the outside network than there are public addresses available then no others will be able to leave the network until another becomes free. This type of NAT is fine for multiple users to use as long as not all users need access to the outside network at once, although it may have problems with a large client base and smaller pool.

Port Address Translation maps multiple private IPv4 addresses to just a few public IP addresses. Pat uses the pair source port and source IP address to keep track of what traffic belongs to what internal client. By using this port number method PAT forwards the response packets to the correct device within the local network. The PAT process also adds a layer of security by validating that the incoming packets were requested. PAT is the most used method

of translation as it doesn't have an upper limit to the amount of users that can leave the local network.

While Dynamic NAT and PAT sound similar, they are quite different in the way that they work. Dynamic NAT uses a one-to-one method, like Static NAT, but does it automatically based on the requests. Pat however doesn't just modify the addresses but also the port number; this is what allows for watch device to use the same addresses without incident.

CONFIGURING NAT

Static NAT: This is used in a one-to-one configuration. This is typically used in servers that need to be accessed from the outside. For example: a web server. In this example, we will use the FastEthernet 0/1 as the inside NAT interface, the interface connecting to our network, and the Serial 0/0/0 interface as the outside NAT interface, the one connecting to our service provider.

```
Router(config)# ip nat inside source static 192.168.0.10 209.165.200.10
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip nat inside
Router(config-if)# interface Serial 0/0/0
Router(config-if)# ip nat outside
```

Static NAT will provide a permanent mapping between the internal and public IP address that was configured. In this example the private IP 192.168.0.10 will always be assigned to 209.165.200.10.

Dynamic NAT: This is used when you have an assigned 'pool' of public IP addresses you want to be automatically assigned per host. Don't use dynamic NAT for servers of anything else that needs to be accessed from an outside network. Many of those devices rely on having a stable address.

In this example, the internal network is 192.168.0.0/24. We also have the pool of public IP addresses from 209.165.200.226 to 209.165.200.240 and our assigned subnet mask is 255.255.255.224. When you configure dynamic NAT, you have to define an ACL to permit only those addresses that are allowed to be translated.

```
Router(config)# ip nat pool NAT-POOL 209.165.200.226 209.165.200.240 netmask
255.255.255.224
Router(config)# access-list 1 permit 192.168.0.0 0.255.255.255
Router(config)# ip nat inside source list 1 pool NAT-POOL
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip nat inside
```

```
Router(config-if)# interface Serial 0/0/0
Router(config-if)# ip nat outside
```

This configuration allows addresses in the 192.168.0.0/24 to be translated to a public IP address in the assigned range. When an inside host makes a request to an outside host, the router dynamically assigns an available IP address from the pool.

Port Address Translation (NAT overload): This is the most used type of NAT. This can be configured in two ways, mostly depending on how many public IP's you have. The first and most used method is if you only have one public IP available. In this case, you will map all your inside hosts to the single IP address. The configuration is almost the same as for dynamic NAT, but this time you specify the outside interface instead of a NAT pool.

```
Router(config)# access list 1 permit 192.168.0.0 0.255.255.255
Router(config)# ip nat inside source list 1 interface serial 0/0/0 overload
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip nat inside
Router(config-if)# interface Serial 0/0/0
Router(config-if)# ip nat outside
```

In this case, the router automatically determines what public IP address to use for the mappings by checking what IP is assigned to the Serial 0/0/0 interface. All the inside addresses are translated to the only public IP address available on your router. Routers are able to recognize the traffic flows by using port numbers, specified by the overload keyword.

The second case is that your ISP gave you more than one public IP addresses, but not enough for a dynamic or static mapping. The configuration is the same as for dynamic NAT, but this time we will add overload for the router to know to use traffic flow identification using port numbers, instead of mapping a private to a public IP address dynamically.

```
Router(config)# ip nat pool NAT-POOL 209.165.200.226 209.165.200.240 netmask
255.255.255.224
Router(config)# access-list 1 permit 192.168.0.0 0.255.255.255
Router(config)# ip nat inside source list 1 pool NAT-POOL overload
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip nat inside
Router(config-if)# interface Serial 0/0/0
Router(config-if)# ip nat outside
```

If you feel sometimes works wrong in your configuration, you can always check the NAT translations and statistics with help of the show commands.

```
Router# show ip nat statistics
```

NETWORK ADDRESS TRANSLATION LAB

Three new networks are being added to the edge of an ISP: Campus A, Campus B, and Campus C. Needing to cross the ISP and keep their private IP scheme, the ISP has given each network a set amount of public IP addresses to implement NAT.

Campus A has 128 hosts and the private IP scheme of 172.16.0.0/24. It has been given the public scheme of 207.120.5.8/28.

Campus B has 500 hosts and the private IP scheme of 10.0.0.0/8 with the public IP scheme of 105.100.0.0/29, but not everyone needs access to the outside networks.

Campus C has over 200 hosts but only the servers need NAT access. It has been given the public IP scheme of 205.109.1.0/29.

Each branch should be using a different kind of NAT, as each branch has only so many IP's as well as has different requirements for the setup.

You must configure each campus router with the correct commands to configure NAT within the address scheme provided. Each interface of the campus routers will need to be configured as well as the private networks within each branch. The ISP router will need the interfaces configured that are connected to the campus branches.

Each router already has routes configured using EIGRP with an ASN of 1. At the end of configuration be sure to test connectivity between all branches as well as across the ISP router. Each campus should be able to ping the ISP router, except for the workstation at campus 'C'.