**NAT** 🡪 **Network Address Translation**

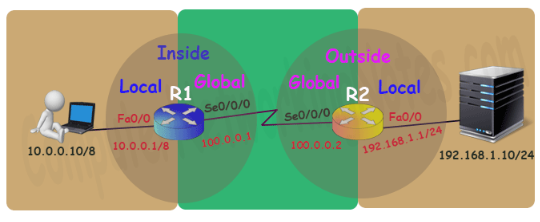
* NAT generally operates on a router or firewall.
* The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required.
* NATis a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table.
* Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. 🡪When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

**TYPES OF NETWORK:**

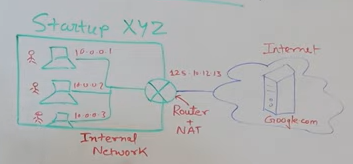
Local network / Global network:

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization.

|  |  |  |
| --- | --- | --- |
| **TERM** |  | **DESCRIPTION** |
| Inside local IP address | Before translation source IP address located inside the local network | An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network. |
| Inside global IP address | After translation source IP address located outside the local network | IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network. |
| Outside global IP address | Before translation destination IP address located outside the remote network | This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation. |
| Outside local IP address | After translation destination IP address located inside the remote network | This is the actual IP address of the destination host in the local network after translation. |



**BENEFIT OF NAT:**

* NAT conserves legally registered IP addresses.
* It provides privacy as the device’s IP address, sending and receiving the traffic, will be hidden.  Because we translate our address into other address (public).
* 

**DISADVANTAGE OF NAT:**

* Translation results in switching path delays.
* Certain applications will not function while NAT is enabled.
* Complicates tunneling protocols such as IPsec.
* Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

**TYPES OF NAT:**

1. Static NAT:

One-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

1. Dynamic NAT:

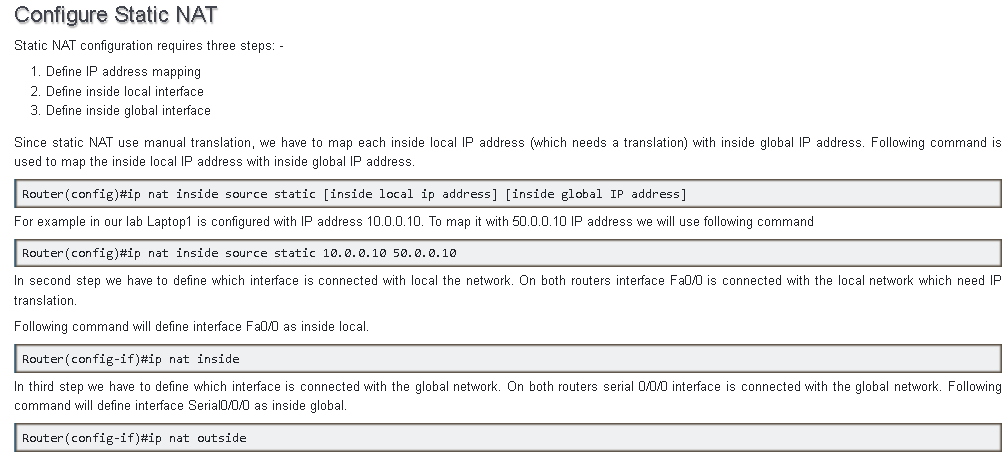
An IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.

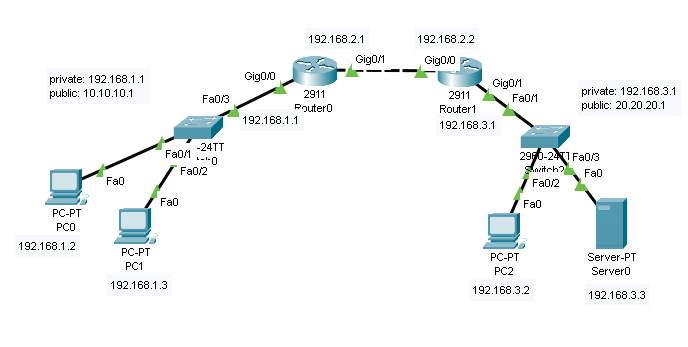
Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT pool is used with the limited number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

1. NAT overload / port address translation (PAT):

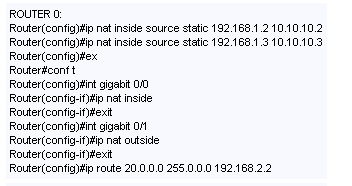
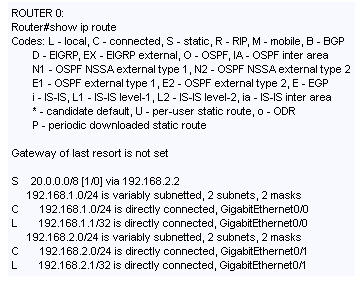
Many local IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global IP address.

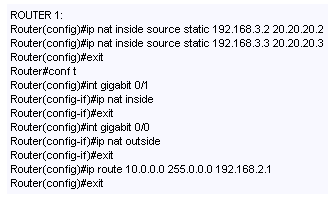
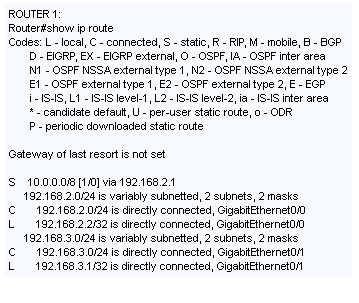
1. **STATIC NAT:**

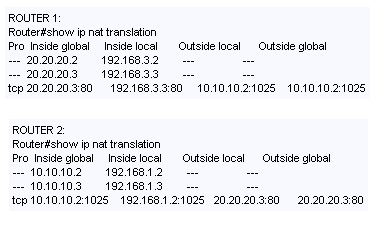




Assign the IP addresses to PC’S, SERVER, and ROUTER statically. Then configure NAT on routers.

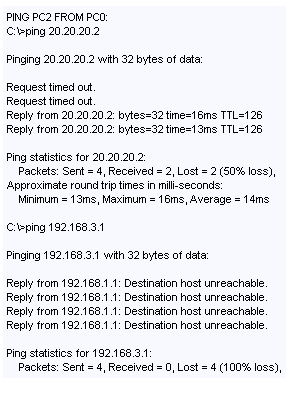


Now if you send packet between two networks then it will failed because of two reasons:

1. No direct access
2. Different public and private address. Router recognize network by publi address but for packet transfer we use private address.

Same scenario with server, To access it from PCs we have to use public address not private one.

But we can ping PC and Server using public address, it recieves all packets and there will be no lost of packets.



1. **DYNAMIC NAT:**

**Configure Dynamic NAT:**

Dynamic NAT configuration requires four steps: -

1. Create an access list of IP addresses which need translation
2. Create a pool of all IP address which are available for translation
3. Map access list with pool
4. Define inside and outside interfaces

**STEP 1:**

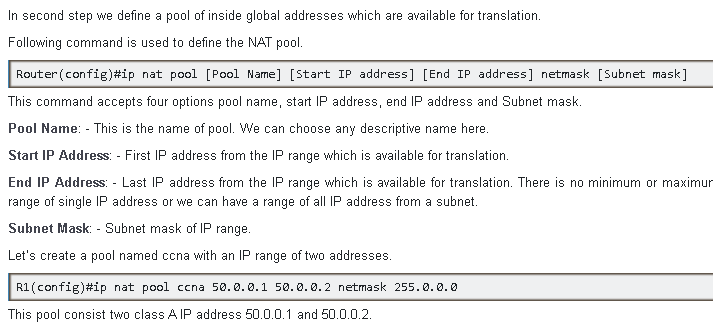
In first step we will create a standard access list which defines which inside local addresses are permitted to map with inside global address.

R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0

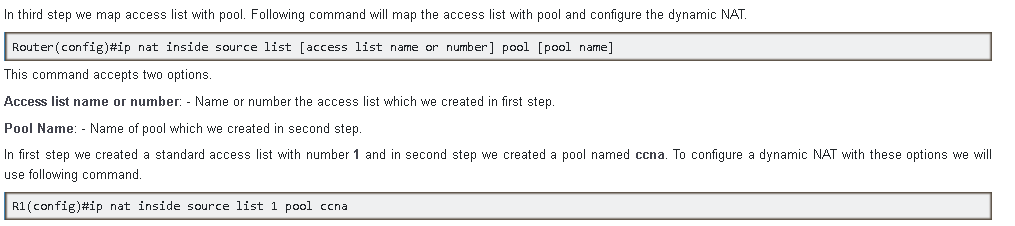
R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0

R1(config)#access-list 1 deny any

**STEP 2:**



**STEP 3:**



**STEP 4:**

