Leonardo Gallego

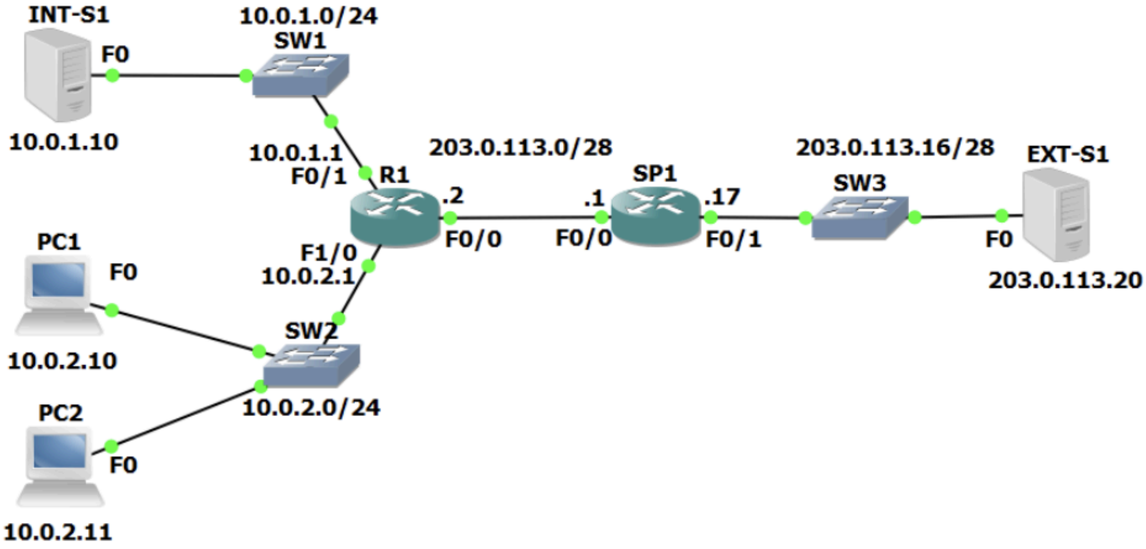
07/12/2025

Today's Networks

- Many industry experts predicted in the early 200's that IPv6 would be ubiquitous within a few years
- It hasn't worked out that way - most enterprises today use RFC 1019 IPv4 addresses with NAT
- RFC 1918 has the security benefit of hiding inside hosts by default (they don't have a publicly routable IP address), plus network engineers have more experience with IPV5 than Ipv6

Nat Types

- **Static NAT**: Permanent 1-to-1 mapping usually between a public and private IP address. Used for servers which must accept incoming connections
- **Dynamic NAT:** uses a pool of public addresses which are given out on an as needed first come first served basis. Usually used for internal hosts which need to connect to the internet but don't accept incoming connections
- **PAT (port Address Translation)** - allows the same public ip address to be reused



Static NAT Scenario

- We have bought the range of public IP addresses 203.0.113.0/28 from our service provider
- 203.0.113.2 is used on the outside interface on our internet edge router R1
- 203.0.113.1 is used as the default gateway address. IT's the SP1 router on the other side of the link
- 203.0.113.3 - 203.0.113.14 remain available
- Int-S1 at 10.0.1.10 is an internal web server which needs to accept incoming connections from the internet
- We need to assign a fixed public IP address to accept incoming connections. We will use the first available address 203.0.113.3
- A static NAT translation is required to translate the public IP address 203.0.113.3 on F0/0 to 10.0.1.10 on F1/0 for incoming connections
- The translation is bidirectional so will also translate 10.0.1.10 to 203.0.113.3 for outbound traffic from the server

Static NAT Configuration

```
R1(config) # int f0/0
R1(config-if)#ip nat outside

R1(config)#int f1/0
R1(config-if) ip nat inside
R1(config)#ip nat inside source static 10.0.1.10 203.0.113.3
```

Inside Local, Inside Global, Outside Local, Outside Global

NAT definitions:

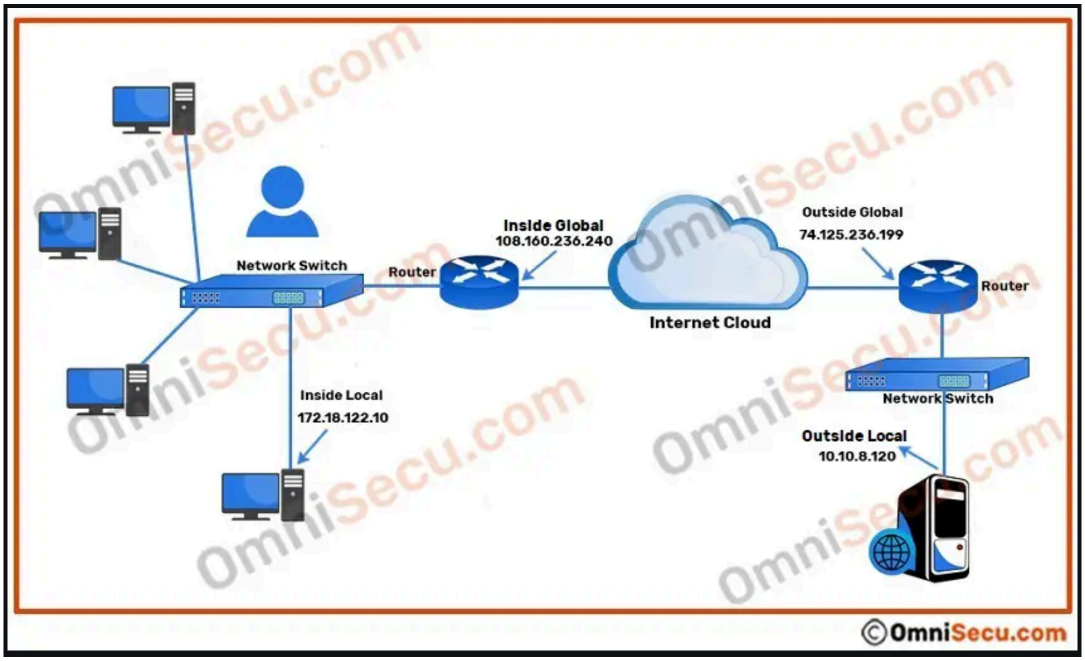
- **Inside local address** - The IP address actually configured on the inside host's operating system
- **Inside Global Address** - The NAT'd address of the inside host as it will be reached by the outside network
- **Outside Local address** - The IP address of the outside host as it appears to the inside network
- **Outside global address -** The IP address assigned to the host on the outside network by the host's owner

Easier said:

- Inside local - your host IP
- inside global - your public IP
- Outside local - remote host IP
- outside global - remote public IP

-

The outside local IP will usually be the same as the outside global IP because they're most likely also using NAT



NAT Verification - Show ip nat translation

Dynamic Nat:

Definition: uses a pool of public addresses which are given out on an as needed first come first served basis. Usually used for internal hosts which need to connect to the internet but don't accept incoming connections

- Traffic is never initiated from th outside so a permanent fix IP address is not necessary, just the next available one

Scenario:
We have bought the range of public IP addresses 203.0.113.0/28 from our service provider

- 203.0.113.2 is used on the outside interface on our internet edge router R1
- 203.0.113.1 is used as the default gateway address. IT's the SP1 router on the other side of the link
- 203.0.113.3 is used for a static NAT translation for the 10.0.1.10 web server
- 203.0.113.4 - 203.0.113.14 remain available

- The hosts in the 10.0.2.0/24 network don't accept incoming connections so they don't need a fixed public IP address with a static NAT translation
- They don't need outbound connectivity to the internet so need to be translated to a public IP address
- We will use the remaining public addresses 203.0.113.4 - 14 as a NAT pool
- The inside hosts will be translated to the public IP addresses on a first come first served basis when they send traffic out
- The first host to send traffic out will be translated to 203.0.113.4, the second host to 203.0.113.5 etc., up to 203.0.113.14 at the end of the pool
- With standard dynamic NAT you need a public IP address for every inside host which needs to communicate with the outside
- If you have 30 hosts, you need 30 public IP addresses
- When all the addresses in the pool have been used, new outbound connections from other inside hosts will fail because there will be no addresses left to translate them to
- These hosts would have to wait for existing connections to be torn down and the translations to be released back into the pool when they time out

Dynamic NAT Configuration

```
R1(config)#int f0/0
R1(config-if)# ip nat outside
R1(config) int f2/0
R1(config-if)# ip nat inside
```

Configure the pool of global addresses

```
R1(config)#ip nat pool Flackbox 203.0.113.4 203.0.113.14 netmask
255.255.255.240
```

Create an access list which references the internal IP addresses we want to translate

```
R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255
```

Associate the access list with the NAT pool to complete the configuration

```
R1(config)# ip nat inside source list 1 pool Flackbox
```

Clear ip nat translation

- Can be used to remove translations from the translation table
- can be useful for troubleshooting
- it's also often required if you want to edit your NAT configuration - the router will not allow changes when there are active translations
- clear ip nat translation * will remove all dynamic translation

```
R1(config-if)# clear ip nat translation
```

```
R1# debug ip Nat
```

PAT

PAT (port Address Translation) - allows the same public ip address to be reused

Issue with Dynamic Nat

- with standard dynamic NAT the insist hosts are translated to public IP addresses on a first come first served basis when they send traffic out
- This requires a public ip address for every inside host which communicates with the outside network
- When all the addresses in the pool have been used, new outbound connections from other inside hosts will fail because there will be no addresses left to translate them to
- In other words It exhausts all available addresses

PAT Address Translation

- Port Address Translation(PAT) is an extension to NAT that permits multiple devices to be mapped to a single public ip address
- With PAt you don't need a public ip address for every inside host
- The router tracks translations by IP address and layer 4 port number
- Because d different inside host are assigned different port numbers, the router knows which host to send return traffic to, even when the public ip address is the same

Dynamic NAT with Overload

- uses PAT to allow more clients to be translated than ip addresses are available in the NAT pool
- IF the NAT pool is 203.0.113.4 to 203.0.113.6 for example, the first 2 host which initiate outbound connections will be translated to 203.0.113.4 and 203.0.113.5
- The 3rd host will be translated to 203.0.113.6 and the router will track which source port number was used in the translation table
- The 4th and 5th etc. hosts will also be translated to 203.0.113.6 but with different source port numbers
- When the return traffic is sent back the router checks the destination port number to see which host to forward to it

Standard Dynamic NAT Configuration

R1(config)# int f0/0
R1(config-if)# ip nat outside
R1(config)# int f2/0
R1(config-if)# ip nat inside

Configure the pool of global addresses

```
R1(config)# ip nat pool Flackbox 203.0.113.4 203.0.113.6 netmask
255.255.255.240
```

Create an access list which references the internal ip addresses we want to translate

```
R1(config)# access-list 1 permit 10.0.2.0 0.0.0.255
```

Associate the access list with the NAT pool to complete the configuration

```
R1(config)# ip nat inside source list 1 pool Flackbox
```

With Overload Configuration:
Associate the access list with the NAT pool to complete the configuration

```
R1(config)# ip nat inside source list 1 pool Flackbox overload
```

PAT with Single IP address

- The last NAT scenario to cover is a small office which has not purchased a range of public IP addresses
- IN this case the outside interface will most likely get its IP address from via DHCP from the service provider
- PAT can be used to allow multiple inside hosts to share the single outside public IP address

PAT with Single IP address Configuration

```
R1(config)# int f0/0
R1(config-if)# ip address dhcp
R1(config-if)# ip nat outside

R1(config)# int f1/0
R1(config-if)# ip nat inside

R1(config)# access-list 1 permit 10.0.2.0 0.0.0.255
```

```
R1(config)# ip nat inside source list 1 interface 10/0 overload
```