NAT Notes – Udemy Course (David Bombal)

Inside Local Inside Global Outside Local Outside Global

3 Types of NAT (Network Address Translation) for CCNA
- Static NAT
- Dynamic NAT
- PAT (Port Address Translation)

Static NAT
- Private IPv4 address (inside local address) → Public IPv4 address (inside global address)
- One-to one mapping
- Useful → access host from outside of the network
  - Ex: webserver
  - Media Server
  - Other local services you want accessible from anywhere
- Not very efficient, use when necessary
- Example 10.10.0.8 becomes 104.191.71.102

Port Address Translation (PAT)
- Multiple private IPv4 addresses → single public IP address
  - Ex: 10.10.0.150:32400 (Plex) → 104.191.70.100 (Public IP address from ATT)
  - Ex: 10.10.0.10:9000 (Portainer) → Public address (access Portainer service from outside home LAN)
- **Uses port numbers to differentiate between different translations**
- Useful for when you only have **1 public IP address, but multiple devices and/or services** to host
- Term: NAT overloading – overloading multiple IP addresses (private IPv4 addresses/port numbers) to a single interface (usually outgoing nat port on edge router – edge of private network and WAN)
- Type of Dynamic NAT (and the most common NAT type)

Dynamic NAT
- Pool of Inside Global Addresses
- Dynamic Allocates IP addresses (as needed)
- No permanent one-to-one mapping
- NAT Translations are automatically created
- NAT Translations are torn down when not needed
- PAT is a type of dynamic mapping with port numbers appended to IP addresses
- Uses Pools of outside local addresses (Pools are setup like with DCHP)
- cmd: ip nat pool NAME BEGIN (address) END (address) netmask 255.255.255.0
- Uses access lists to indicate the list of inside local source addresses

IP nat Pools – this is where the outside local addresses

Access-list indicate the list of inside local source addresses

Demo in Packet Tracer: Static NAT

NAT configured on R2
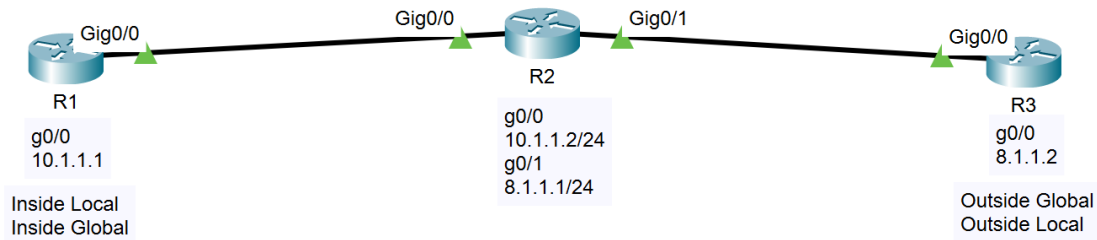
R1 has a default route to R2
R1 R2 R3 have no routing protocols running
R3 has no default route
R2(config)#ip nat inside static (inside local) (inside global)
R2(config)#ip nat inside static 10.1.1.1 8.1.1.5
With the above command R1's inside local address (10.1.1.1) is translated to the inside global address (8.1.1.5), which is on the same subnet as R3. Thus, R1 can now ping R3 through a Static NAT translation
We also need to apply 'nat inside' to an interface (closest to internal LAN) and nat outside to an interface facing the internet / external network
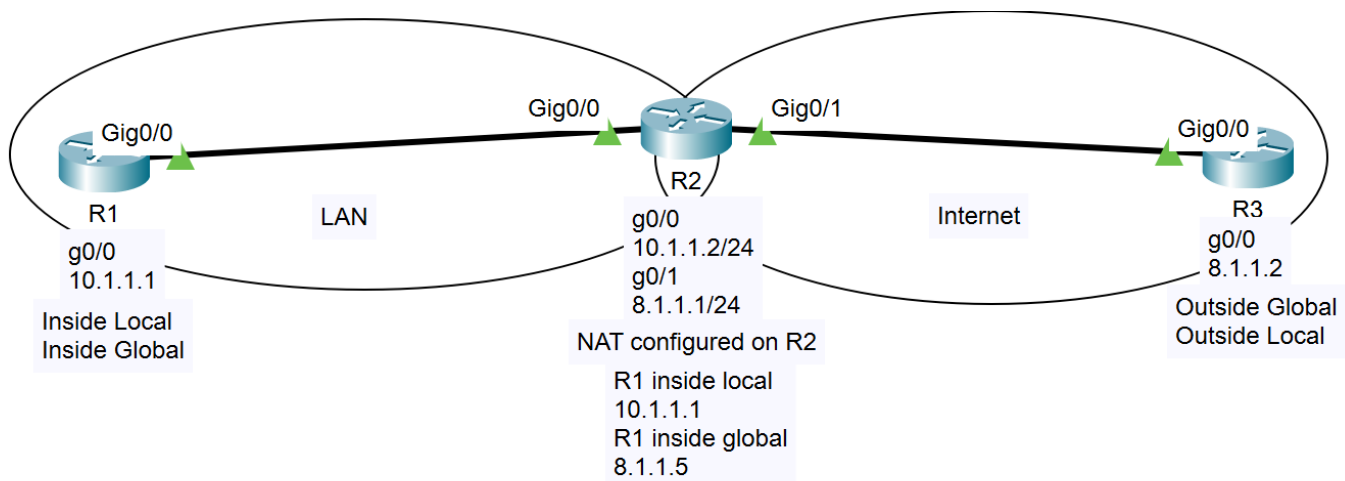R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config)#int g0/1
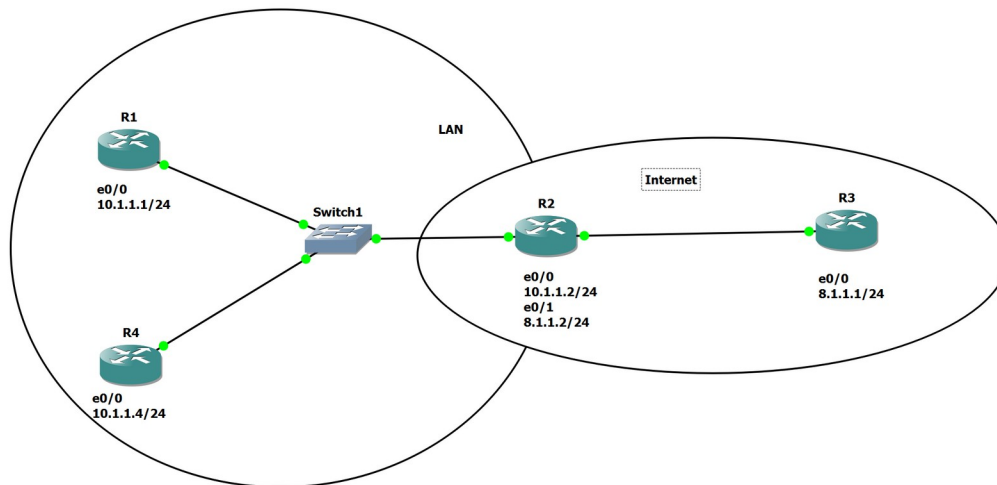R2(config-if)#ip nat outside

Show command
```
R2#sh ip nat translations
Pro  Inside global      Inside local      Outside local      Outside
global
---  8.1.1.5            10.1.1.1          ---                ---
```


When we imagine this setup think of R3 as a host connected to the internet attempting to access a website/service hosted on a device in your LAN (so R1 is essentially a server)

Demo in Packet Tracer: Dynamic NAT

1. Configure "inside" and "outside" interfaces
R2 e0/0 – Nat inside
    e0/1 – Nat outside

2. Create an Access List (standard) permitting local addresses
R2(config)#access-list 1 permit 10.1.1.0 0.0.0.255

3. Create a NAT Pool
R2(config)#ip nat pool [NAME] [BEGIN] (address) [END] (address) netmask 255.255.255.0
R2(config)#ip nat pool NATPOOL 8.1.1.5 8.1.1.10 netmask 255.255.255.0

4. Assign the ACL (created in Step 2) to the Nat Pool (created in step 3)
R2(config)#ip nat inside source list 1 pool NATPOOL

Issues with Dynamic NAT
There is a one-to-one mapping between our inside and outside ip addresses, but there are only so many
addresses available in our pool. The solution is NAT overloading

<u>Demo in Packet Trace: (Port Address Translation) PAT / NAT Overloading</u>
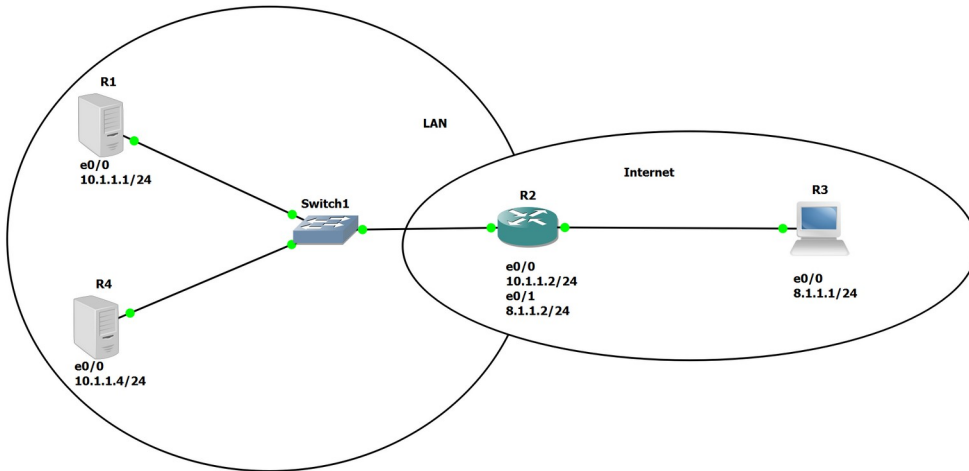
In this example our two server in the LAN need to be accessible by the PC (R3), so the two switches are going to be NATed to the single IP address – 8.1.1.2 (outgoing port on R2). This will be done with PAT/ NAT overloading. Overloading means that multiple addresses can use one interface on the edge router.

1. Configure "inside" and "outside" interfaces
R2 e0/0 – Nat inside
    e0/1 – Nat outside

2. Create an Access List (standard) permitting local addresses on 10.1.1.0/24
R2(config)#access-list 1 permit 10.1.1.0 0.0.0.255

3. Assign the ACL (created in Step 2) to Outside interface with overload appended to have multiple ips on one interface
R2(config)#ip nat inside source list 1 interface ethernet 0/0 overload
The key here is the command "overload" which allows more than 1 IP addresses to be "overloaded" on a single interface

```
R2#sh ip nat tr
Pro Inside global      Inside local      Outside local      Outside global
tcp 8.1.1.2:56637      10.1.1.1:56637    8.1.1.1:23         8.1.1.1:23
tcp 8.1.1.2:40759      10.1.1.4:40759    8.1.1.1:23         8.1.1.1:23
```

Source Address Translation

Typically NATing devices on your internal network (RFC 1918 address), so they can be translated by NAT and become accessible via a device outside your internal network (outside local/global address)

Private LAN (Inside Local) Address is NATed (translated) into a routable address (inside global), then the internet-routable inside global address can communicate with devices outside the LAN (outside global addresses)