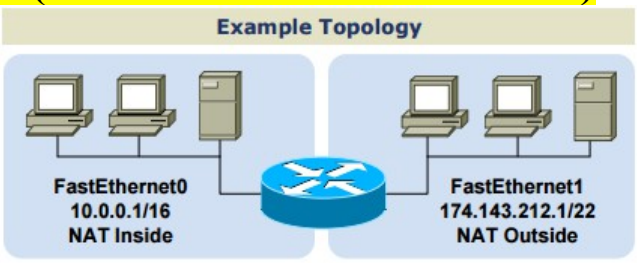
NAT (Network Address Translation)

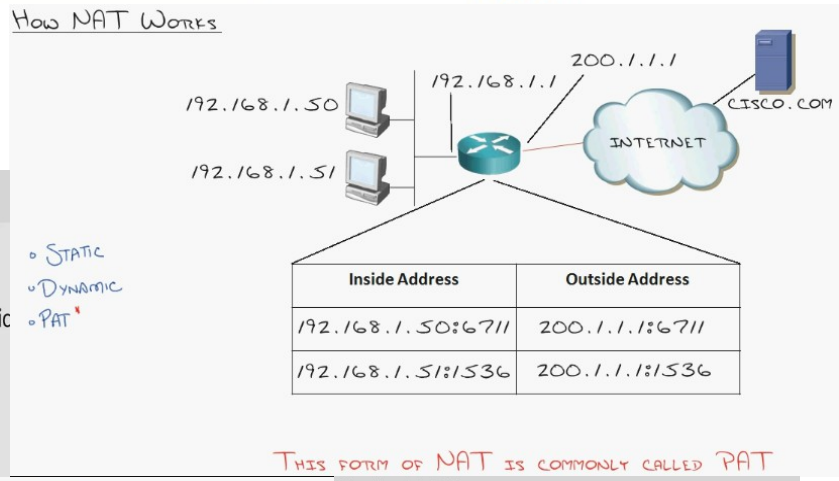


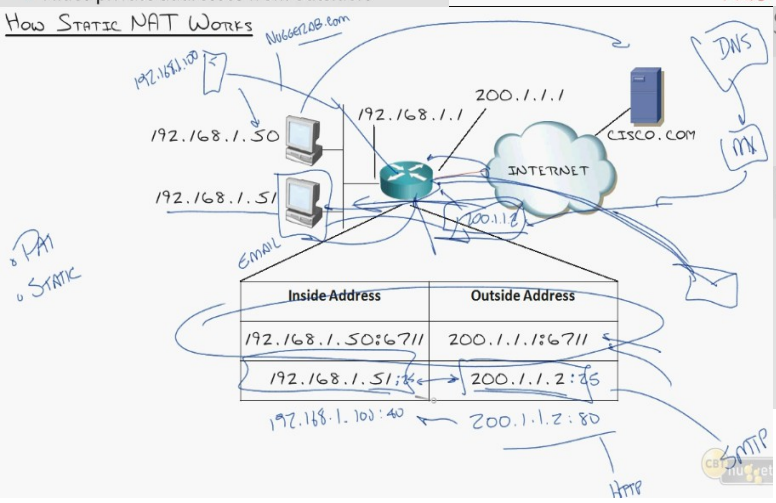
Address Classification	
Inside Local	An actual address assigned to an inside host
Inside Global	An inside address seen from the outside
Outside Global	An actual address assigned to an outside host
Outside Local	An outside address seen from the inside

		Perspective	
		Local	Global
Location	Inside	Inside Local	Inside Global
	Outside	Outside Local	Outside Global

Introduction to NAT

- Separates LAN from WAN and provides accessibility to the outside world
- Translates RFC1918 space addresses into public addresses
- Provides security
- Helps reduce public IP address consumption
- Hides private addresses from outsiders





Static NAT

- One to one mapping
- One private host requires a public IP address
- Usually deployed at server end

Dynamic NAT

- Many to many mapping
- One private host requires a public IP address obtained from a pool of available addresses.
- Usually deployed at client end
- Easier from the perspective of scalability

PAT

- Port Address Translation
- One to many mapping
- One public address can provide multiple host connections
- Usually deployed at client end
- Easier from the perspective of scalability

Configuring Static NAT

- Configuration commands
  - Router(config-if)# ip nat inside
  - Router(config-if)# ip nat outside
  - Router(config)# ip nat inside source static <private address> < public address>

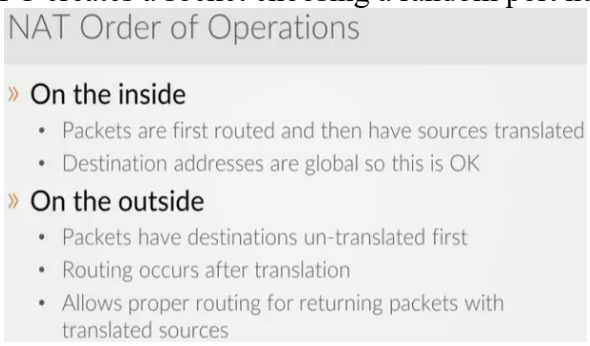
Configuring Dynamic NAT

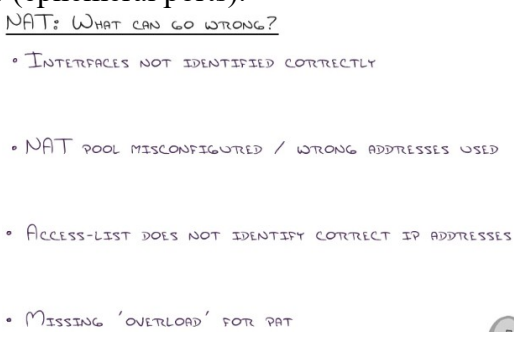
- Configuration commands
  - Router(config-if)# ip nat inside
  - Router(config-if)# ip nat outside
  - Router(config# access-list < acl no> <permit | deny > <source-address> <wildcard mask>
  - Router(config)# ip nat pool <name> <start-ip> <end-ip> netmask <subnet mask>
  - Router(config)# ip nat inside source list < acl no> pool <name>

Configuring PAT

- Configuration commands
  - Router(config-if)# ip nat inside
  - Router(config-if)# ip nat outside
  - Router(config# access-list < acl no> <permit | deny > <source-address> <wildcard mask>
  - Router(config)# ip nat pool <name> <start-address> <end-address> netmask < subnet mask>
  - Router(config)# ip nat inside source list < acl no> pool <name> overload

PC creates a socket choosing a random port number (ephemeral ports).





Configuration:

Define the traffic to match:

R(config)#access-list 10 permit 10.0.0.0 0.0.255.255 !(ACL to match)

Static NAT: (Note: two way NAT. Just like a port-forward so be careful)

R(config)#ip nat inside source static 10.0.0.19 192.0.2.1

R(config)#ip nat outside source static 174.143.212.133 10.0.0.47

Dynamic NAT:

R(config)#ip nat pool MyPool 192.0.2.1 192.0.2.254 prefix-length 24 !(Public IP pools)

R(config)#ip nat inside source list 10 pool MyPool !(actual NAT rule)

R(config)#ip nat inside source static 10.0.0.42 192.0.2.42 !(can be combined with static)

PAT:

R(config)#ip nat inside source static tcp 10.0.0.3 80 192.0.2.1 80

R(config)#ip nat inside source static tcp 10.0.0.3 443 192.0.2.1 443

R(config)#ip nat inside source static tcp 10.0.0.10 3389 192.0.2.1 3389

R(config)#ip nat inside source static tcp 10.0.0.11 3389 192.0.2.1 3390

R(config)#ip nat inside source list 10 pool MyPool overload

OR

R(config)#ip nat inside source list 10 interface FastEthernet 0/0 overload

Identify interfaces: (Note: should be the last step, especially in a production network)

R(config)#int fa0/0

R(config-if)#ip address dhcp !(ISP assigned IP for external interface)

R(config-if)#ip nat outside

R(config)#int fa0/1

R(config-if)#ip address 192.168.1.1

R(config-if)#ip nat nat inside

How long the NAT translations or NAT Entries are kept for?

udp: 1. udp timer is 5 minute before the nat translation timesout.

tcp: 1. syn sent, but never received a syn/ack back so nat translation timeout is 1 min.
2. syn and syn/ack received, but then only keepalives were seen by the router for 24 hours it will remove the nat entry. 3. someone who is finishing the session is sending tcp FIN or tcp RST to kill the session, router will still the nat entry for another 1 min. 4. if there was no graceful session end (e.g. cables disconnected), router if it doesn't see the keepalives for a 1 min will remove the entry.

NAT Translations Tuning

```
ip nat translation tcp-timeout <seconds>
ip nat translation udp-timeout <seconds>
ip nat translation max-entries <number>
```

Inside Destination Translation

```
! Create a rotary NAT pool
ip nat pool LoadBalServers 10.0.99.200 10.0.99.203 prefix-length 24 type rotary
!
! Enable load balancing across inside hosts for incoming traffic
ip nat inside destination list 12 pool LoadBalServers
```

Verifications and TSHOOT:

```
sh ip nat trans
sh run | inc ip nat
sh ip nat trans verbose
sh ip nat stat
clear ip nat trans *
debug ip nat
```