Introduction to Network Address Translation

Network Infrastructure Workshop

Last updated October2019

Network Address Translation

- NAT has become a commonly used technique for prolonging the use of IPv4 on today's Internet

Problems with IPv4

Shortage of IPv4 addresses

Allocation of the last IPv4 addresses was for the year 2005

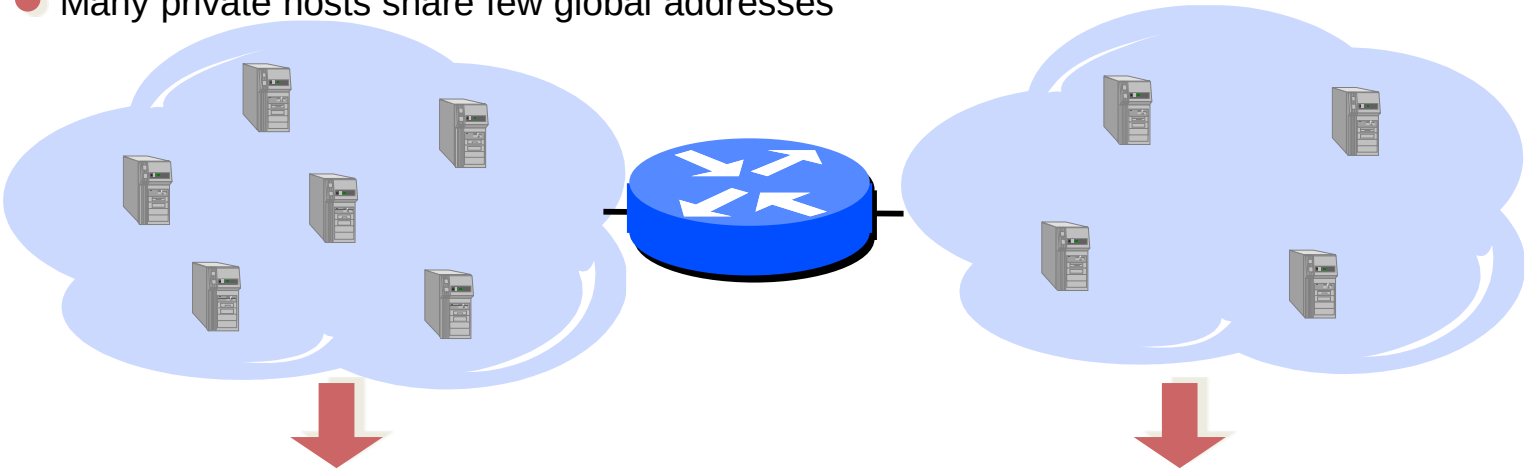
Address classes were replaced by usage of CIDR, but this is not sufficient

- Short term solution
  - NAT: Network Address Translator

- Long term solution
  - IPv6 = IPng (IP next generation)
  - Provides an extended address range

Network Address Translation

- Translates between local addresses and public ones
- Many private hosts share few global addresses



Private Network

- Uses private address range (local addresses)
- Local addresses may not be used externally

Public Network

- Uses public addresses
- Public addresses are globally unique

NAT Addressing Terms

- **Inside Local**

The term "inside" refers to an address used for a host inside an enterprise. It is the actual IP address assigned to a host in the private enterprise network.

Inside Global

NAT uses an inside global address to represent the inside host as the packet is sent through the outside network, typically the Internet.

A NAT router changes the source IP address of a packet sent by an inside host from an inside local address to an inside global address as the packet goes from the inside to the outside network.

NAT Addressing Terms

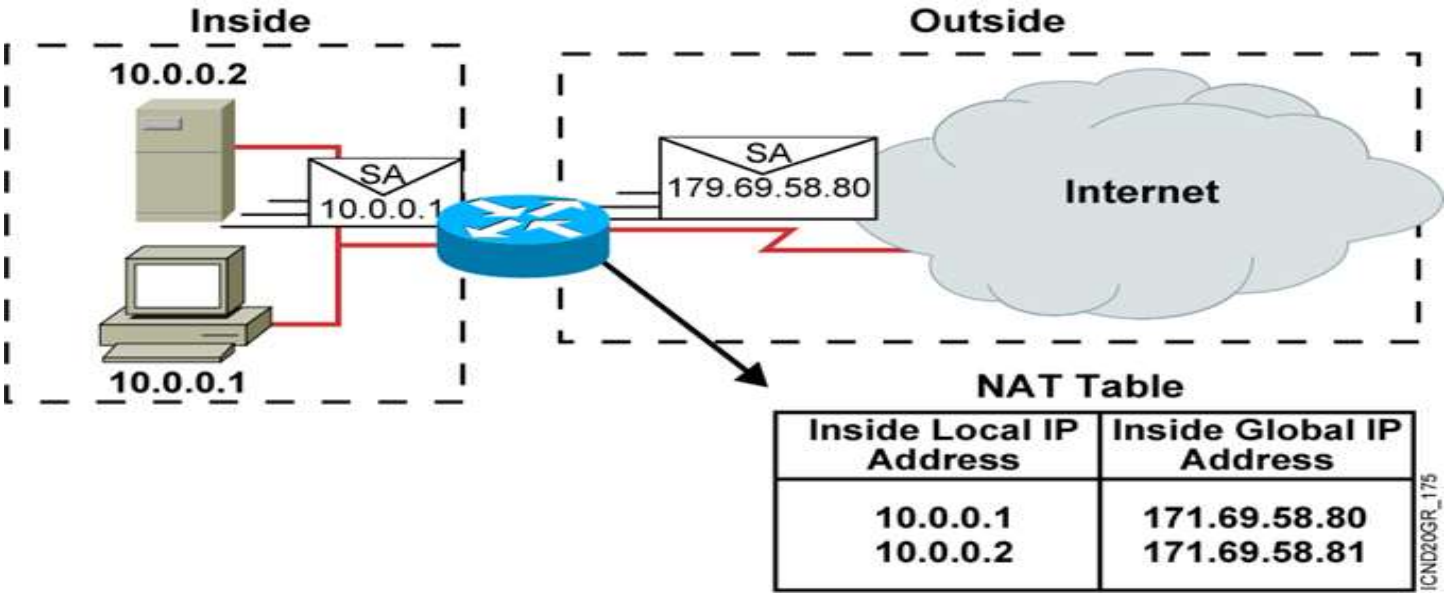
Outside Global

- The term “outside” refers to an address used for a host outside an enterprise, the Internet.
- An outside global is the actual IP address assigned to a host that resides in the outside network, typically the Internet.

Outside Local

- NAT uses an outside local address to represent the outside host as the packet is sent through the private network.
- This address is outside private, outside host with a private address

Network Address Translation



- An IP address is either local or global.
- Local IP addresses are seen in the inside network.

Types Of NAT

- There are different types of NAT that can be used, which are
  - Static NAT
  - Dynamic NAT
  - Overloading NAT with PAT (NAPT)

Static NAT

- Static NAT - Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.

- In static NAT, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110.

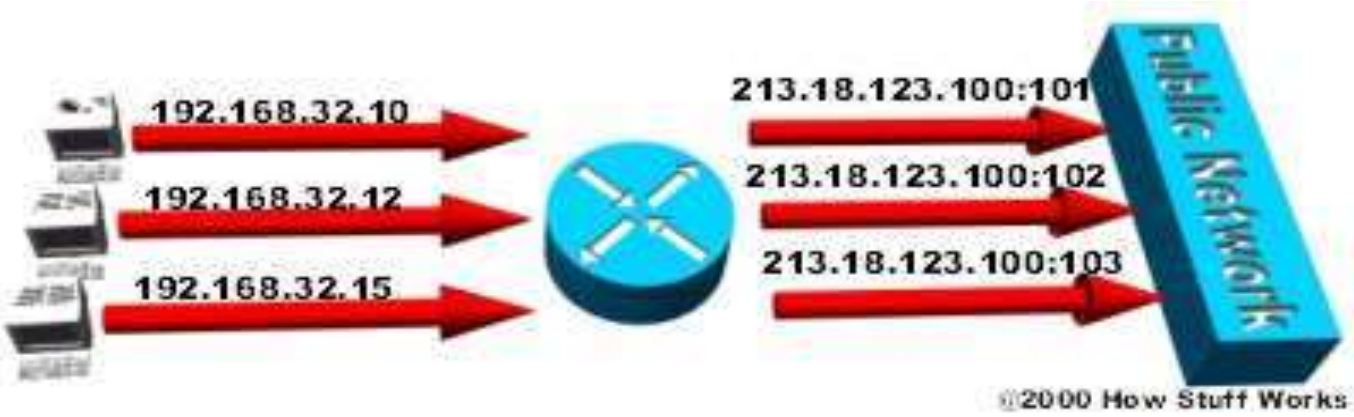
Dynamic NAT

- Dynamic NAT - Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.

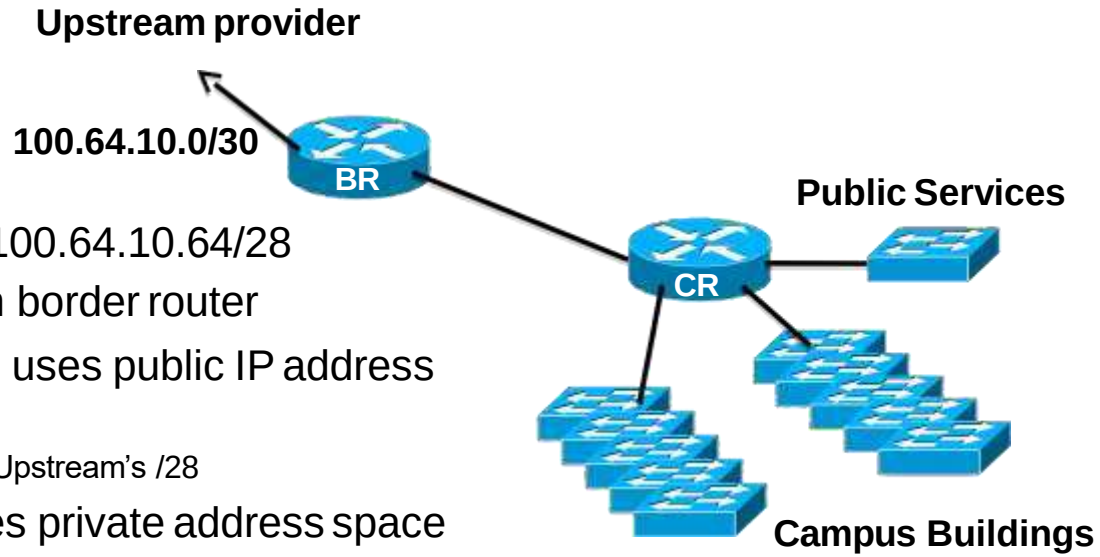
- In dynamic NAT, the computer with the IP address 192.168.32.10 will translate to the first available address in the range from 213.18.123.100 to 213.18.123.150.

Overloading NAT with PAT (NAPT)

- Overloading - A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. This is known also as PAT (Port Address Translation), single address NAT or port-level multiplexed NAT.
- In overloading, each computer on the private network is translated to the same IP address (213.18.123.100), but with a different port number assignment..



Campus Use Case: Simple



- Upstream provides 100.64.10.64/28
- NAT implemented on border router
- Public Services LAN uses public IP address block
  - 100.64.10.72/29 from Upstream's /28
- Rest of Campus uses private address space
  - 192.168.0.0/16
  - NAT'ed to 100.64.10.64/29

Typical Cisco configuration (1)

- NAT Configuration set up on Border Router
- Define the address range we want to NAT

```
ip access-list  extended  NATplus
 deny   ip 100.64.10.0 0.0.0.255 any
 deny   ip 192.168.0.0  0.0.255.255 192.168.0.0  0.0.255.255
 permit ip 192.168.0.0  0.0.255.255 any
 deny   ip any any log
```

- This says:
  - Don't NAT any of 100.64.10.0/24
  - Don't NAT when source and destination addresses are both internal
  - NAT internal source to any external destination
  - Anything that doesn't match is logged to catch "errors"

Typical Cisco configuration (2)

- Define the external interface we want to NAT to:

```
interface GigabitEthernet 0/1
 description Link to ISP
 ip address 100.64.10.2 255.255.255.252
 ip nat outside
!
```

- Define the internal interface we want to NAT from:

```
interface  GigabitEthernet  0/2
 description Link to Campus Core Switch
 ip address 192.168.255.1 255.255.255.252
 ip nat inside
!
```

Typical Cisco configuration (3)

- Modifying the translation timeouts:

```
ip nat translation dns-timeout 60
ip nat translation icmp-timeout 180
ip nat translation udp-timeout 300
ip nat translation finrst-timeout 60
ip nat translation tcp-timeout 3600
```

- This will
  - Set the translation timeouts for DNS to 60 seconds, ICMP to 180 seconds, UDP to be 300 seconds, FIN/RST to be 60 seconds (all Cisco defaults), and TCP to 3600 seconds (from 86400 seconds default)
    - Timeout is when there is no more traffic using that mapping
  - Other translation timeout options are available in Cisco IOS too but the above are the most commonly used

Typical Cisco configuration (4a)

- Activating the NAT on ONE IPv4 address

```
ip nat inside source list NATplus interface Gigabit 0/1 overload
```

- This will
  - match the NATplus list for traffic going from Gigabit 0/2 to Gigabit 0/1
  - Overload means use NAPT (one to many mapping using TCP/UDP ports)
    - NAPT will use the IP address of the Gigabit 0/1 port to map all the internal addresses to
- Campus traffic will appear as though it is all originated from the 100.64.10.2 address

Typical Cisco configuration (4b)

- Activating the NAT on an IPv4 address pool
- First create the public address pool:

```
ip nat pool CAMPUS 100.64.10.64 100.64.10.67 prefix-length 29
```

  - Which defines the pool CAMPUS having 4 IP public IP addresses out of the 100.64.10.64/28 address block given to the campus
- Now enable NAT

```
ip nat inside source list NATplus pool CAMPUS overload
```

  - Which will match all traffic in the NATplus list translating it into the address pool CAMPUS