Network Address Translation (Basic)

Safwan Muntasir (Sufi)
Networking Enthusiast

Before starting this study material, in case if you didn't check, it is recommended to go through the study material named "ACL Basic"

Contents

Back to Contents

Introduction

Network Address Translation (NAT) was first proposed in 1992 by Phil Karn and Kathleen Greene. It was first implemented in the Cisco PIX Firewall in 1994. NAT quickly became a popular way to conserve IPv4 addresses, and is now used in most routers and firewalls.

NAT is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. The technique was originally used to bypass the need to assign a new address to every host when a network was moved, or when the upstream Internet Service provider was replaced, but could not route the network's address space.

Why do we need NAT?

- **To conserve IPv4 addresses:** The Ipv4 address space is limited, and NAT allows us to use multiple devices behind a single public IP address. This is specially important for home networks, where we may have devices connected to the internet, such as computers, smartphones, tablets, etc. NAT ensures that none of the IP networks are reused.
- **To improve security:** NAT can help to improve security by hiding the private IP addresses of devices on the network. This makes it more difficult for attackers to target specific devices.
- **To control traffic:** NAT can be used to control traffic that enters and leaves the network. This can be used to block unwanted traffic and to improve performance.

Back to Contents

IPv4 Address Shortage Solutions

To overcome IPv4 address shortage, two solutions are applied-

1. **Short Term Solutions:** By using IPv4 addresses.
- Private addressing. (RFC 1918)
- Network Address Translation (NAT)
- Subnetting and Classless Interdomain Routing (CIDR)

2. **Long Tern Solutions:** By using IPv6 addresses.
- Increase the size of the IP address to 128 bits.
- Assigning unique address ranges to every organization connected to the Internet.

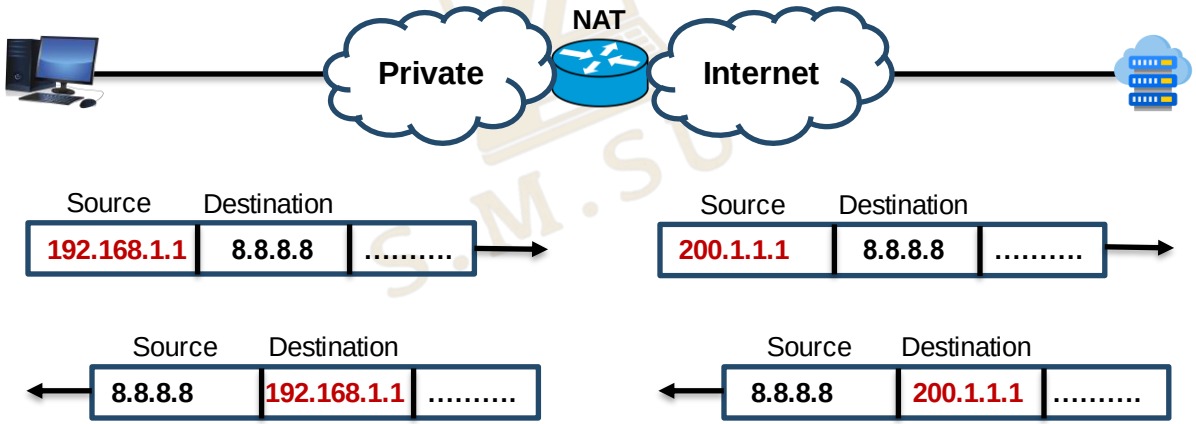
Public and Private IPv4 Address

Public IPv4 Address:
- Used on public network (Internet)
- Recognized on Internet
- Globally unique and Registered address
- Given by the service provider (from IANA)
- Pay to service provider (or IANA)

Private IPv4 Address:
- Used with the LAN or within the organization
- Given by the administrator
- Unique within the network or organization
- Not recognized on Internet
- Free / Unregistered IP

What is NAT?

NAT, defined in RFC 3022, is 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. NAT generally operates on a routers, firewalls and servers.

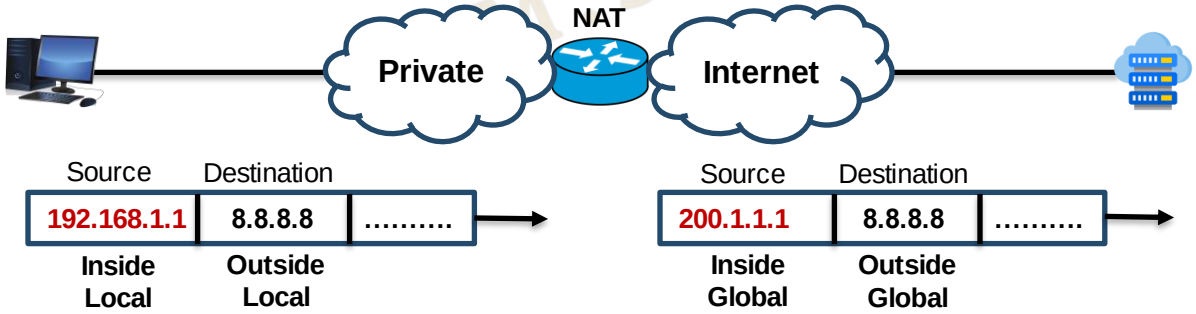


Back to Contents

Types

There are three main types of NAT-

1. **Static NAT**: Static NAT maps a single private IP address to a single public IP address. This is typically used for servers that need to be accessible from the public Internet. This is one-to-one mapping provides a consistent and permanent mapping.
2. **Dynamic NAT**: Dynamic NAT maps a pool of private IP addresses to a pool of public IP addresses. This is typically used for clients that need to access the public Internet, but do not need to be directly accessible from the public Internet. The mapping is temporary and based on the first-come, first-served principle.
3. **NAT Overload**: Also known as Port Address Translation (PAT). PAT is a type of dynamic NAT that uses a single public IP address to represent multiple private IP addresses. This is done by using different port numbers to distinguish between the different private IP addresses. PAT is the most common type of NAT used today. This is one-to-many mapping.



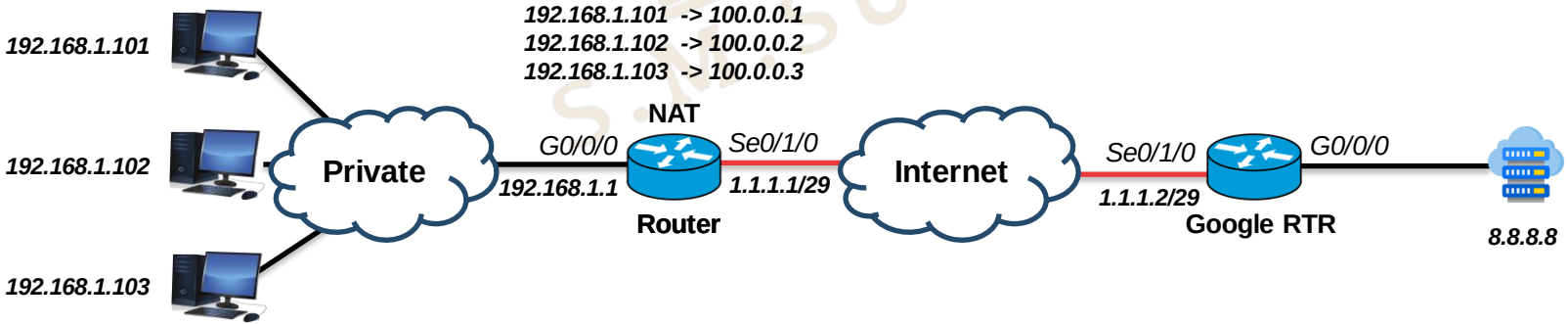
Static NAT

- One-to-one mapping. Maps a single private IP address to a single public IP address.
- A consistent and permanent mapping.
- Not suitable for network where a large number of host exist.
- Commands for selecting inside/outside interface-

  'Router(config)# interface <interface name>'

  'Router(config-if)# ip nat <inside/outside>'
- Commands for static nat-

  'Router(config)# ip nat <inside> source <static> <inside local ip address> <inside global ip address>'



Back to Contents

Static NAT

```
Router(config)#interface g0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se0/1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

```
Router(config)#ip nat ?
  inside   Inside address translation
  outside  Outside address translation
  pool     Define pool of addresses
Router(config)#ip nat inside ?
  source  Source address translation
Router(config)#ip nat inside source ?
  list    Specify access list describing local addresses
  static  Specify static local->global mapping
Router(config)#ip nat inside source static ?
  A.B.C.D  Inside local IP address
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
Router(config)#ip nat inside source static 192.168.1.101 ?
  A.B.C.D  Inside global IP address
Router(config)#ip nat inside source static 192.168.1.101 100.0.0.1
Router(config)#ip nat inside source static 192.168.1.102 100.0.0.2
Router(config)#ip nat inside source static 192.168.1.103 100.0.0.3
Router(config)#end
```

Layer 3: IP Header Src. IP: 192.168.1.101, Dest. IP: 8.8.8.8 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 100.0.0.1, Dest. IP: 8.8.8.8 ICMP Message Type: 8
Layer 2: Ethernet II Header 0001.426A.CC69 >> 0000.0CBA.A701	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0/0	Layer 1: Port(s): Serial0/1/0

1. The routing table finds a routing entry to the destination IP address.
2. The device decrements the TTL on the packet.
3. The packet is going from an inside to an outside network. The device looks up its NAT table for necessary translations.
4. The NAT table has a matched static entry for the source local address.
5. The device translates the packet from local to global addresses with the matched entry.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  100.0.0.1         192.168.1.101      ---                ---
---  100.0.0.2         192.168.1.102      ---                ---
---  100.0.0.3         192.168.1.103      ---                ---
```

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 100.0.0.1:5       192.168.1.101:5    8.8.8.8:5          8.8.8.8:5
icmp 100.0.0.1:6       192.168.1.101:6    8.8.8.8:6          8.8.8.8:6
icmp 100.0.0.2:5       192.168.1.102:5    8.8.8.8:5          8.8.8.8:5
icmp 100.0.0.2:6       192.168.1.102:6    8.8.8.8:6          8.8.8.8:6
icmp 100.0.0.3:5       192.168.1.103:5    8.8.8.8:5          8.8.8.8:5
icmp 100.0.0.3:6       192.168.1.103:6    8.8.8.8:6          8.8.8.8:6
```

Back to Contents

Dynamic NAT

- One-to-one mapping done automatically. Maps a pool of private IP addresses to a pool of public IP addresses.
- The mapping is temporary and based on the first-come, first-served principle.
- This is typically used for clients that need to access the public Internet, but do not need to be directly accessible from the public Internet.
- If all the pooled IP addresses are in use, the router simply discard the packet.
- Commands for selecting inside/outside interface-

  'Router(config)# interface <interface name>'

  'Router(config-if)# ip nat <inside/outside>'
- Commands for defining private addresses via standard access-lists-

  'Router(config)# access-list <acl no> <permit/deny> <source ip> <source wcm>'
- Commands for defining private addresses via extended access-lists-

  'Router(config)# access-list <acl no> <permit/deny> <protocol> <source ip> <wcm> <dest. Ip> <wcm> <operator> <port/service>'
- Commands for creating nat pool for converted public addresses-

  'Router(config)# ip nat pool <pool name> <starting public ip> <ending public ip> netmask <subnet mask>'
- ***Commands for dynamic nat-***

  'Router(config)# ip nat <inside> source <list> <acl no> pool <pool name>'

Dynamic NAT

```
Router(config)#interface g0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se0/1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

```
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool ?
  WORD  Pool name
Router(config)#ip nat pool mypool ?
  A.B.C.D  Start IP address
Router(config)#ip nat pool mypool 100.0.0.1 ?
  A.B.C.D  End IP address
Router(config)#ip nat pool mypool 100.0.0.1 100.0.0.3 netmask ?
  A.B.C.D  Network mask
Router(config)#ip nat pool mypool 100.0.0.1 100.0.0.3 netmask 255.255.255.0
Router(config)#
Router(config)#ip nat inside source ?
  list    Specify access list describing local addresses
  static  Specify static local->global mapping
Router(config)#ip nat inside source list 10 ?
  interface  Specify interface for global address
  pool       Name pool of global addresses
Router(config)#ip nat inside source list 10 pool mypool ?
  overload  Overload an address translation
  <cr>
Router(config)#ip nat inside source list 10 pool mypool
```

Layer 3: IP Header Src. IP: 192.168.1.101, Dest. IP: 8.8.8.8 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 100.0.0.1, Dest. IP: 8.8.8.8 ICMP Message Type: 8
Layer 2: Ethernet II Header 0005.5EC0.D8E1 >> 00D0.D3B3.C94A	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0/0	Layer 1: Port(s): Serial0/1/0

1. The routing table finds a routing entry to the destination IP address.
2. The device decrements the TTL on the packet.
3. The packet is going from an inside to an outside network. The device looks up its NAT table for necessary translations.
4. The packet matches an inside source list and creates a new entry for source local address.
5. The device translates the packet from local to global addresses with the matched entry.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  100.0.0.1         192.168.1.101      ---                ---
---  100.0.0.2         192.168.1.102      ---                ---
---  100.0.0.3         192.168.1.103      ---                ---
```

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 100.0.0.1:8       192.168.1.101:8    8.8.8.8:8          8.8.8.8:8
icmp 100.0.0.1:9       192.168.1.101:9    8.8.8.8:9          8.8.8.8:9
icmp 100.0.0.2:3       192.168.1.102:3    8.8.8.8:3          8.8.8.8:3
icmp 100.0.0.2:4       192.168.1.102:4    8.8.8.8:4          8.8.8.8:4
icmp 100.0.0.3:3       192.168.1.103:3    8.8.8.8:3          8.8.8.8:3
icmp 100.0.0.3:4       192.168.1.103:4    8.8.8.8:4          8.8.8.8:4
```

Back to Contents

NAT Overload

- Also known as Port Address Translation (PAT).
- Maps a pool of private IP addresses to a single public IP address but different port numbers.
- The port numbers used in PAT are typically in the rage of 0124 to 65535. These are assigned uniquely and randomly.
- As PAT uses only one public ip for translation, so the starting and ending ip address will be the same.
- Commands for selecting inside/outside interface-

  'Router(config)# interface <interface name>'

  'Router(config-if)# ip nat <inside/outside>'
- Commands for defining private addresses via standard access-lists-

  'Router(config)# access-list <acl no> <permit/deny> <source ip> <source wcm>'
- Commands for defining private addresses via extended access-lists-

  'Router(config)# access-list <acl no> <permit/deny> <protocol> <source ip> <wcm> <dest. Ip> <wcm> <operator> <port/service>'
- Commands for creating nat pool for converted public addresses-

  'Router(config)# ip nat pool <pool name> <starting public ip> <ending public ip> netmask <subnet mask>'
- ***Commands for nat overload/pat-***

  'Router(config)# ip nat <inside> source <list> <acl no> pool <pool name> overload'

NAT Overload

```
Router(config)#interface g0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se0/1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

```
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool ?
  WORD  Pool name
Router(config)#ip nat pool mypool ?
  A.B.C.D  Start IP address
Router(config)#ip nat pool mypool 100.0.0.1 ?
  A.B.C.D  End IP address
Router(config)#ip nat pool mypool 100.0.0.1 100.0.0.1 netmask ?
  A.B.C.D  Network mask
Router(config)#ip nat pool mypool 100.0.0.1 100.0.0.1 netmask 255.255.255.255 ?
  <cr>
Router(config)#ip nat pool mypool 100.0.0.1 100.0.0.1 netmask 255.255.255.255
Router(config)#
Router(config)#ip nat inside source ?
  list     Specify access list describing local addresses
  static   Specify static local->global mapping
Rou    (config)#ip nat inside source list 10 ?
  interface  Specify interface for global address
  pool       Name pool of global addresses
Router(config)#ip nat inside source list 10 pool mypool ?
  overload  Overload an address translation
  <cr>
Router(config)#ip nat inside source list 10 pool mypool overload
```

Layer 3: IP Header Src. IP: 192.168.1.103, Dest. IP: 8.8.8.8 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 100.0.0.1, Dest. IP: 8.8.8.8 ICMP Message Type: 8
Layer 2: Ethernet II Header 0005.5ECD.D26D >> 0005.5E6D.D0A5	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0/0	Layer 1: Port(s): Serial0/1/0

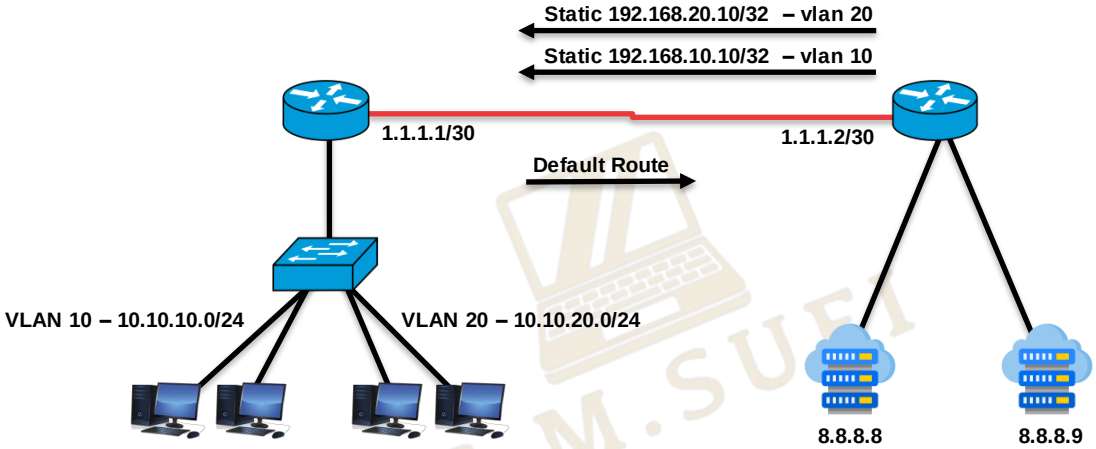
1. The routing table finds a routing entry to the destination IP address.
2. The device decrements the TTL on the packet.
3. The packet is going from an inside to an outside network. The device looks up its NAT table for necessary translations.
4. The packet matches an inside source list and creates a new entry for source local address.
5. The device translates the packet from local to global addresses with the matched entry.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  100.0.0.1         192.168.1.101      ---                ---
---  100.0.0.2         192.168.1.102      ---                ---
---  100.0.0.3         192.168.1.103      ---                ---
```

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 100.0.0.1:1024    192.168.1.102:1    8.8.8.8:1          8.8.8.8:1024
icmp 100.0.0.1:1025    192.168.1.102:2    8.8.8.8:2          8.8.8.8:1025
icmp 100.0.0.1:1026    192.168.1.102:3    8.8.8.8:3          8.8.8.8:1026
icmp 100.0.0.1:1027    192.168.1.102:4    8.8.8.8:4          8.8.8.8:1027
icmp 100.0.0.1:1028    192.168.1.103:1    8.8.8.8:1          8.8.8.8:1028
icmp 100.0.0.1:1029    192.168.1.103:2    8.8.8.8:2          8.8.8.8:1029
icmp 100.0.0.1:1030    192.168.1.103:3    8.8.8.8:3          8.8.8.8:1030
icmp 100.0.0.1:1031    192.168.1.103:4    8.8.8.8:4          8.8.8.8:1031
```

Back to Contents

Exercise 1



Only PCs from VLAN 10 can ping Server 8.8.8.8 and PCs from VLAN 20 can ping Server 8.8.8.9. Solve this exercise with ACL and NAT.

Thank You

Feel free to reach out to me for any **suggestions** or **feedback** via **LinkedIn** or **Mail**

 www.github.com/smsufi

 www.linkedin.com/in/smsufi

 safwanm.cse@gmail.com

References

- https://en.wikipedia.org/wiki/Network_address_translation
- https://www.techtarget.com/searchnetworking/definition/Network-Address-Translation-NAT#:~:text=A%20Network%20Address%20Translation%20(NAT,IP%20addresses%20an%20organization%20needs.
- https://www.geeksforgeeks.org/network-address-translation-nat/
- https://www.comptia.org/content/guides/what-is-network-address-translation
- https://www.youtube.com/@SIKANDARshaik/playlists