Network Address Translation (NAT)

NAT

- NAT maps Private IPs to Public IPs.
- A short term solution to the problem of the depletion of IP addresses
- It is required because of shortage of IPv4 Address.
- Whatever connects directly into Internet must have public (globally unique) IP address
- So Private IP addresses can be used within a private network
- Three address ranges are reserved for private usage
  - 10.0.0.0/8
  - 172.16.0.0/16 to 172.31.0.0/16
  - 192.168.0.0/24 to 192.168.255.0/24
- A private IP is mapped to a Public IP, when the machine has to access the Internet

NAT

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagram's are replaced at the boundary of a private network
- NAT is a method that enables hosts on private networks to communicate with hosts on the Internet.
- NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

List of Situations when NAT is used:

- When you need to connect to the Internet and your hosts don't have globally unique IP addresses.
- When you've changed to a new ISP that requires you to renumber your network.
- When you need to merge two intranets with duplicate addresses

List of Situations when NAT is used:

- When you need to connect to the Internet and your hosts don't have globally unique IP addresses.
- When you've changed to a new ISP that requires you to renumber your network.
- When you need to merge two intranets with duplicate addresses

NAT Names

Names	Meaning
Inside Local	Source host inside address before translation typically an RFC 1918 address
Outside Local	Address from which source host is known on the Internet. This is usually the address of the router interface connected to ISP—the actual Internet address.
Inside Global	Source host address used after translation to get onto the Internet. This is also the actual Internet address.
Outside Global	Address of outside destination host. The real Internet address.

Translation Modes

- Dynamic Translation (IP Masquerading)
- Static Translation
- Load Balancing Translation
- Network Redundancy Translation

Dynamic Translation (IP Masquerading)

- Network Address and Port Translation (NAPT)
- Map an unregistered IP address to a registered IP address from out of a pool of registered IP addresses.
- large number of internal users share a single external address.
- NAT only prevents external hosts from making connections to internal hosts.

Static Translation

- Allow one-to-one mapping between local and global addresses.
- A block external addresses are translated to a same size block of internal addresses
  - Firewall just does a simple translation of each address.
- Port forwarding - map a specific port to come through the Firewall rather than all ports.
- Useful to expose a specific service on the internal network to the public network

Load Balancing Translation

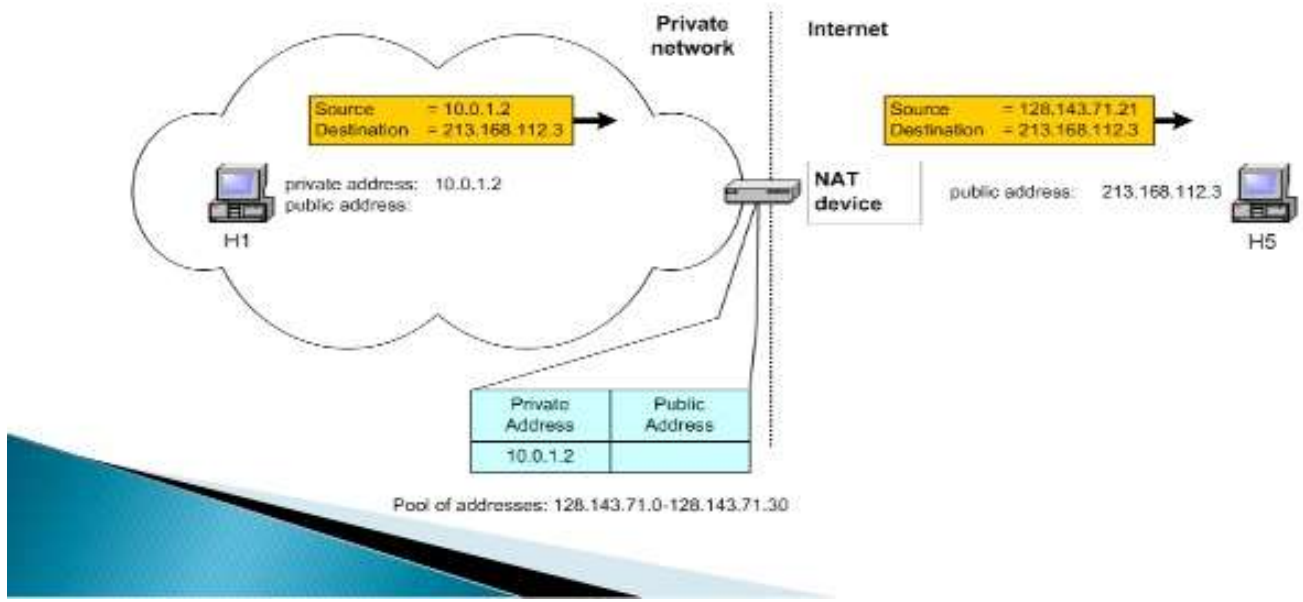
- Maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different source ports.
- *Port Address Translation (PAT) which is also* commonly referred to as *NAT Overload.*
- PAT allows you to permit thousands of users to connect to the Internet using only one real global IP address.
- Only works for stateless protocols (like HTTP)

Network Redundancy Translation

- Multiple internet connections are attached to a NAT Firewall that it chooses.
- Uses based on bandwidth, congestion and availability.
- Can be used to provide automatic fail-over of servers or load balancing.
- Firewall is connected to multiple ISP with a masquerade for each ISP and chooses which ISP to use based on client load
  - kind of like reverse load balancing
  - Adead ISP will be treated as a fully loaded one and the client will be routed through another ISP.

Pooling of IP Addresses

- **Scenario:** Corporate network has many hosts but only a small number of public IP addresses.

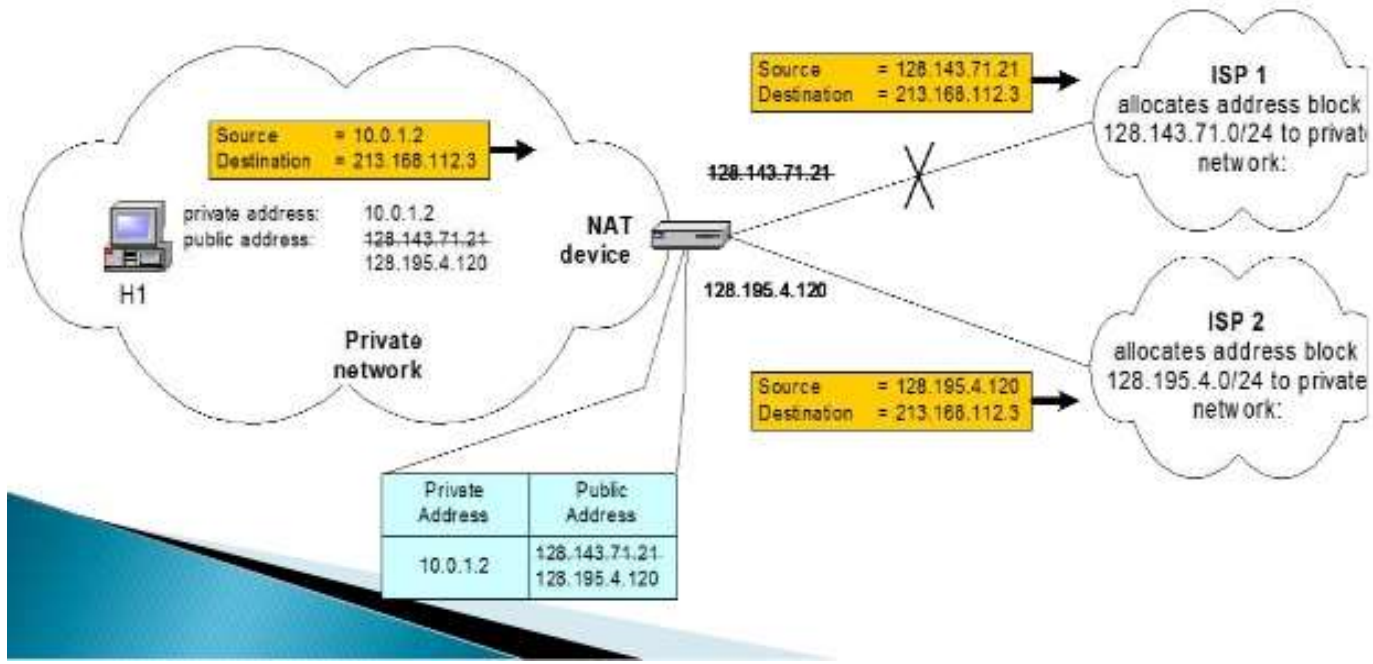


Pooling of IP Addresses

- **NAT solution:**
  - Corporate network is managed with a private address space.
  - NAT device, located at the boundary between the corporate network and the public Internet, manages a pool of public IP addresses.
  - When a host from the corporate network sends an IP datagram to a host in the public Internet, the NAT device picks a public IP address from the address pool, and binds this address to the private address of the host.

Supporting Migration between Network Service Providers

- **Scenario:** In CIDR, the IP addresses in a corporate network are obtained from the service provider. Changing the service provider requires changing all IP addresses in the network.

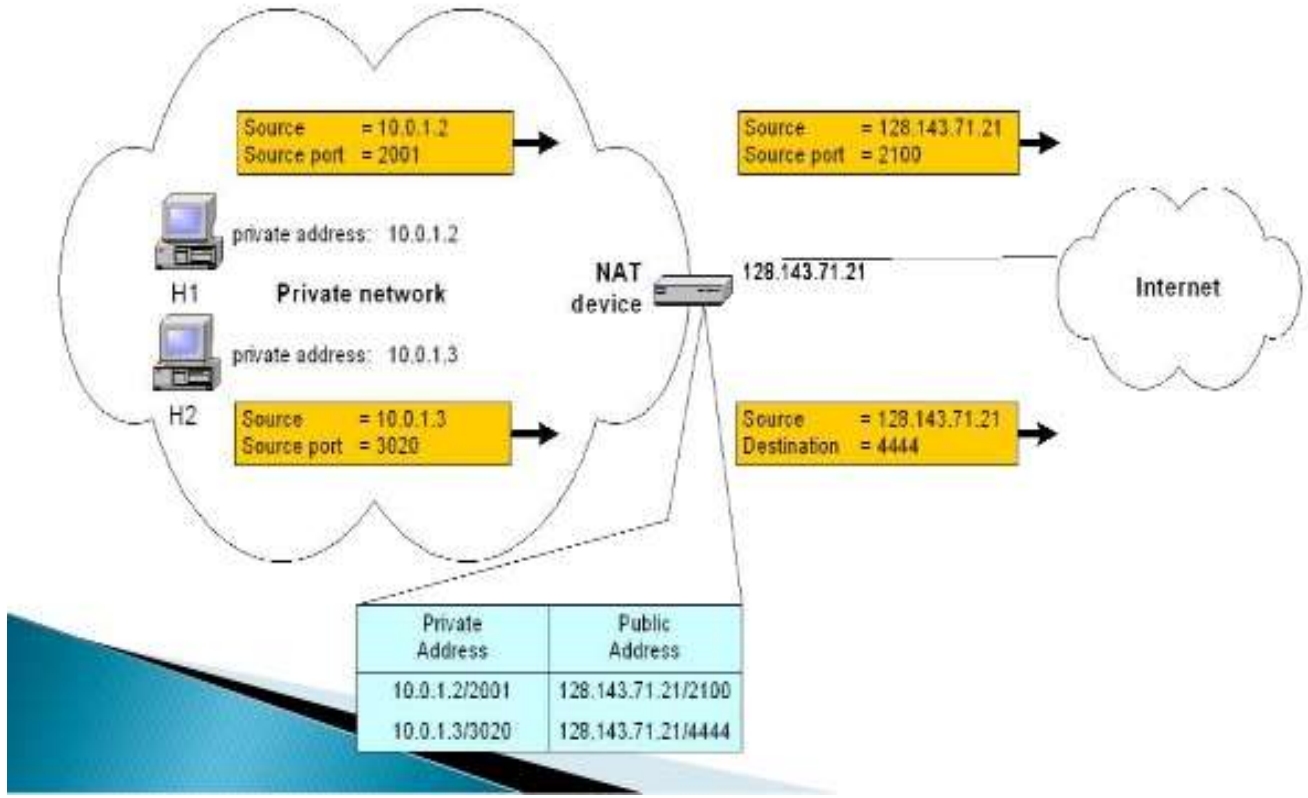


Supporting Migration between Network Service Providers

- **NAT solution:**
  - Assign private addresses to the hosts of the corporate network.
  - NAT device has static address translation entries which bind the private address of a host to the public address.
  - Migration to a new network service provider merely requires an update of the NAT device. The migration is not noticeable to the hosts on the network.
- **Note:**
  - The difference to the use of NAT with IP address pooling is that the mapping of public and private IP addresses is static.

IP Masquerading

- **Scenario:** Single public IP address is mapped to multiple hosts in a private network.

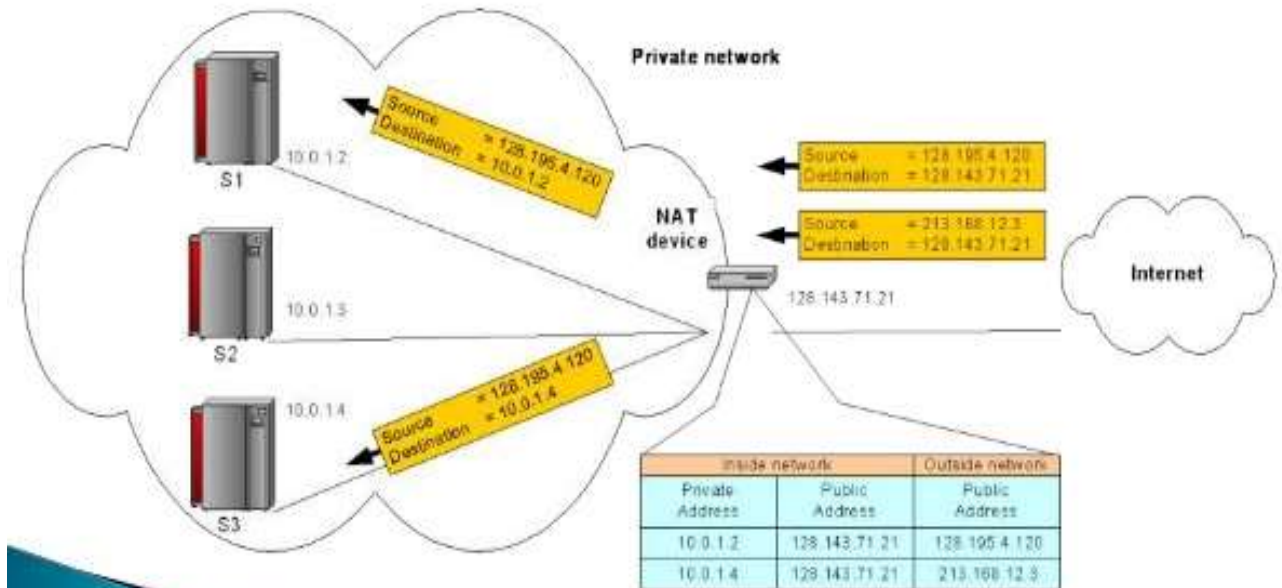


IP Masquerading

- **NAT solution:**
  - Assign private addresses to the hosts of the corporate network.
  - NAT device modifies the port numbers for outgoing traffic.

Load Balancing of Servers

- **Scenario:** Balance the load on a set of identical servers, which are accessible from a single IP address



Load Balancing of Servers

- **NAT solution:**
  - Here, the servers are assigned private addresses.
  - NAT device acts as a proxy for requests to the server from the public network.
  - The NAT device changes the destination IP address of arriving packets to one of the private addresses for a server.
  - A sensible strategy for balancing the load of the servers is to assign the addresses of the servers in a round-robin fashion.

NAT Advantages

- Increases flexibility when connecting to the Internet.
- Eliminates address renumbering as a network evolves.
- Remedies address overlap events.
- Conserves legally registered addresses.

Services that NAT has problems with

1. H.323, CUSeeMe, VDO Live – video teleconferencing applications
2. Xing – Requires a back channel
3. Rshell – used to execute command on remote Unix machine – back channel
4. IRC – Internet Relay Chat – requires a back channel
5. PPTP – Point-to-Point Tunneling Protocol
6. SQLNet2 – Oracle Database Networking Services
7. FTP – Must be RFC-1631 compliant to work
8. ICMP – sometimes embeds the packed address info in the ICMP message
9. IPSec – used for many VPNs
10. IKE – Internet Key Exchange Protocol
11. ESP – IP Encapsulating Security Payload

NAT Applications

- Hardware and software firewalls.
- Routers.
- Proxy servers
  - RAS server that is a simple router/firewall

END