Network Address Translation (NAT)

Relates to Lab 7.
Module about private networks and NAT.

Private Network

- Private IP network is an IP network that is not directly connected to the Internet

- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique

- Generally, private networks use addresses from the following experimental address ranges (non-routable addresses):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
Private Addresses

Network Address Translation (NAT)

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams 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.
Basic operation of NAT

- NAT device has address translation table

Main uses of NAT

- Pooling of IP addresses
- Supporting migration between network service providers
- IP masquerading
- Load balancing of servers
Pooling of IP addresses

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

- **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

• Also called: Network address and port translation (NAPT), port address translation (PAT).

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

• NAT solution:
  – Assign private addresses to the hosts of the corporate network
  – NAT device modifies the port numbers for outgoing traffic

---

IP masquerading

<table>
<thead>
<tr>
<th>Private Address</th>
<th>Public Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.2/2001</td>
<td>128.143.71.21/2100</td>
</tr>
<tr>
<td>10.0.1.3/3020</td>
<td>128.143.71.21/4444</td>
</tr>
</tbody>
</table>

Private network

H1

H2

NAT device

Internet

Source = 10.0.1.2
Source port = 2001

Source = 10.0.1.3
Source port = 3020

Source = 128.143.71.21
Source port = 2100

Destination = 4444
Load balancing of servers

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

- **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.
Concerns about NAT

• **Performance:**
  – Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum
  – Modifying port number requires that NAT boxes recalculate TCP checksum

• **Fragmentation**
  – Care must be taken that a datagram that is fragmented before it reaches the NAT device, is not assigned a different IP address or different port numbers for each of the fragments.

• **End-to-end connectivity:**
  – NAT destroys universal end-to-end reachability of hosts on the Internet.
  – A host in the public Internet often cannot initiate communication to a host in a private network.
  – The problem is worse, when two hosts that are in a private network need to communicate with each other.
Concerns about NAT

- IP address in application data:
  - Applications that carry IP addresses in the payload of the application data generally do not work across a private-public network boundary.
  - Some NAT devices inspect the payload of widely used application layer protocols and, if an IP address is detected in the application-layer header or the application payload, translate the address according to the address translation table.

NAT and FTP

- Normal FTP operation
NAT and FTP

- NAT device with FTP support

NAT and FTP

- FTP in passive mode and NAT.
Configuring NAT in Linux

- Linux uses the Netfilter/iptables package to add filtering rules to the IP module

![Diagram of NAT process]

Configuring NAT with iptable

- **First example:**
  ```
  iptables -t nat -A POSTROUTING -s 10.0.1.2 -j SNAT --to-source 128.143.71.21
  ```
- **Pooling of IP addresses:**
  ```
  iptables -t nat -A POSTROUTING -s 10.0.1.0/24 -j SNAT --to-source 128.128.71.0–128.143.71.30
  ```
- **ISP migration:**
  ```
  iptables -t nat -R POSTROUTING -s 10.0.1.0/24 -j SNAT --to-source 128.195.4.0–128.195.4.254
  ```
- **IP masquerading:**
  ```
  iptables -t nat -A POSTROUTING -s 10.0.1.0/24 -o eth1 -j MASQUERADE
  ```
- **Load balancing:**
  ```
  iptables -t nat -A PREROUTING -i eth1 -j DNAT --to-destination 10.0.1.2–10.0.1.4
  ```