Proxy Server and Network Address Translator
Introduction

• What is a proxy server?
  ➢ Acts on behalf of other clients, and presents requests from other clients to a server.
  ➢ Acts as a server while talking with a client, and as a client while talking with a server.
• Commonly used HTTP proxy server:
  ➢ Squid
    ▪ available on all platforms.

What is it really?

• It is a server that sits between a client application (Web browser), and a real server.
  ➢ It intercepts all requests to the real server to see if it can fulfill the requests itself.
  ➢ If not, it forwards the request to the real server.
• Mainly serves two purposes:
  ➢ Improve performance
    ▪ Can dramatically improve performance for a group of users.
    ▪ It saves all the results of requests in a cache.
    ▪ Can greatly conserve bandwidth.
  ➢ Filter requests
    ▪ Prevent users from accessing a specific set of web sites.
    ▪ Prevent users for accessing pages containing some specified strings.
    ▪ Prevent users from accessing video files (say).

Anonymous Proxy Servers

• Hide the user’s IP address, thereby preventing unauthorized access to user’s computer through the Internet.
• All requests to the outside world originate with the IP address of the proxy server.
• Very convenient for group subscription:
  ➢ On-line journals.
  ➢ Digital library.
Where it is located?

Functions of a HTTP Proxy

- **Request forwarding**
  - Primary function.
  - Acts as a rudimentary firewall.
- **Access control**
  - Allow or deny accesses, based on
    - Contents
    - Location
- **Cache management**
  - Efficient utilization of bandwidth.
  - Faster access.
What is NAT?

- Allows a single device (router or a dedicated box) to act as an agent between the Internet (public network) and a local (private) network.
  - Tries to address the IP address distribution problem.
  - RFC 1631.
  - Only one unique IP address is required to represent an entire group of computers.
  - Several variations possible.
Private Addresses

Basic operation of NAT

- **NAT device has address translation table**
Various Forms of NAT

- **Static NAT**
  - Used to map an unregistered IP address to a registered IP address.
  - One-to-one mapping.
    - $N$ registered addresses for $N$ machines.

- **Dynamic NAT**
  - Used to map an unregistered IP address to a registered IP address.
  - From a given pool of registered IP addresses.
  - Addresses are assigned dynamically.
    - Any number of internal computers.
    - A limit $N$ to the number communicating at a time.

Various Forms of NAT (contd.)

- **Overloading**
  - A special form of dynamic NAT.
  - Used to map multiple unregistered IP addresses to a single registered IP address by using different ports.
    - Also called port address translation (PAT).
    - Each computer on the private network gets translated to the same IP address, but with a different port number assignment.
  - Widely used.
NAT Overloading ....

- Utilizes the multiplexing feature of TCP/IP stack.
  - A computer maintains several concurrent connections with a remote computer, using different port numbers.
- The header of a TCP/IP packet contains:
  - Source IP address (32 bit)
  - Source port number (16 bit)
  - Destination IP address (32 bit)
  - Destination port number (16 bit)
  - The combination of above four elements define a TCP/IP connection.

- Notations:
  - **Stub domain**: the internal or the private network.
  - **Address translation table (ATT)**: maintained by router/NAT for address and port mapping.
- Easy to implement dynamic NAT.
  - Address translation table need only contain IP address mappings.
    - Private to public, and vice versa.
    - No port numbers needed.
How NAT overloading works?

• The scenario:
  ➢ Internal network has non-routable IP addresses.
  ➢ NAT-enabled router contains a registered IP address assigned by IANA.
  ➢ An internal host X tries to connect to, say, an outside Web server.
  ➢ The router receives the packet from X.

➢ The router will now:
  ▪ Save IP address and port number from X’s packet to an ATT.
  ▪ In the packet, replace the IP address with the router’s IP address.
  ▪ Replace the port number with a port number from the ATT (look for match). For new connection, generate a unique port number.
When a packet comes back.
- Its destination port is used to search ATT.
- Source IP address and port numbers can be obtained.
- Addresses changed accordingly.

The Address Translation Table (ATT) looks like:

<table>
<thead>
<tr>
<th>Source Computer</th>
<th>Source IP address</th>
<th>Source port number</th>
<th>NAT IP address</th>
<th>NAT port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10.5.17.112</td>
<td>500</td>
<td>203.11.16.5</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>10.5.17.85</td>
<td>75</td>
<td>203.11.16.5</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>10.23.10.5</td>
<td>2480</td>
<td>203.11.16.5</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>10.22.5.118</td>
<td>1120</td>
<td>203.11.16.5</td>
<td>4</td>
</tr>
</tbody>
</table>
Capability Limit of a NAT

- **Maximum number of concurrent translations:**
  - Mainly determined by the size of the memory to store the ATT.
  - Typical entry in the ATT takes about 160 bits.
  - Memory size of 8 Mbyte will support about
    \[
    8 \times 1024 \times 1024 \times 8 / 160 = 4,19,000
    \]
    concurrent translations.

Which addresses to use inside?

- **Private address classes.**
  - Set aside by IANA an non-routable.
  - These addresses are considered unregistered.
  - Routers discard these addresses, if used as destination.
    - A packet from a host with a private unregistered address can reach a registered destination host, but not the reverse.
The Private Address Classes

- **Class A** (one)
  - 10.0.0.0 to 10.255.255.255
- **Class B** (sixteen)
  - 172.16.0.0 to 172.31.255.255
- **Class C** (256)
  - 192.168.0.0 to 192.168.255.255

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.
Pooling of IP addresses

- 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.

- This migration is not noticeable to the hosts on the network.

**Note:**

- The difference to the use of NAT with IP address pooling is that in the present case mapping of public and private IP addresses is static.

### Supporting Migration

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
<th>Public Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.2</td>
<td>128.143.71.21</td>
<td>128.195.4.120</td>
</tr>
<tr>
<td>128.195.4.120</td>
<td>128.143.71.21</td>
<td>128.143.71.21</td>
</tr>
</tbody>
</table>

**ISP 1** allocates address block 128.143.0/24 to private network.

**ISP 2** allocates address block 128.195.0/24 to private network.
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.

<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>
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.

---

**Load balancing of servers**

Diagram showing private and public networks with NAT device routing traffic to different servers.

---

**Private network**

<table>
<thead>
<tr>
<th>Server</th>
<th>Public Address 1</th>
<th>Private Address 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>128.143.71.21</td>
<td>10.0.1.2</td>
</tr>
<tr>
<td>S2</td>
<td>128.143.71.21</td>
<td>10.0.1.3</td>
</tr>
<tr>
<td>S3</td>
<td>128.143.71.21</td>
<td>10.0.1.4</td>
</tr>
<tr>
<td>S4</td>
<td>128.143.71.21</td>
<td>10.0.1.5</td>
</tr>
</tbody>
</table>

**Internet**

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP 1</th>
<th>Destination IP 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.143.71.21</td>
<td>128.143.71.21</td>
<td>128.143.71.21</td>
</tr>
</tbody>
</table>
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.

Other Benefits of NAT

- **Use of NAT automatically creates a firewall between the internal and external networks.**
  - NAT will only allow connections that has originated from within the internal network.
  - An outside host cannot initiate a connection with an internal host.
- **Inbound mapping requires static NAT.**
Is NAT a Proxy Server?

- The answer is “NO”.
  - NAT is transparent to both source and destination hosts. But a proxy server is not transparent.
  - NAT is a layer 3 (network) protocol. In contrast, a proxy server works at layer 4 (transport) or higher.