Lecture 12.5: Naming (cont)

Midterm MONDAY
Lecture 12.5 Overview

- Discovering addresses (DHCP/ARP)
- Network address translation (NAT)
Whence come IP Addresses?

- You already have a netblock from the days when you called Jon Postel and asked for them (e.g. BBN)

- You get a netblock from another provider
  - E.g. buy service from Sprint and get a /24 from one of their address blocks

- You get a netblock directly from a routing registry
  - ARIN: North America, APNIC (Asia Pacific), RIPE (Europe), LACNIC (Latin America), AFRINIC (Africa)
  - Registries get address from IANA (Internet Assigned Numbers Authority)
How Do You And I Get One?

• Well from your provider!

• But how do you know what it is?

• Manual configuration
  ♦ They tell you and you type that number into your computer (along with the default gateway, DNS server, etc.)

• Automated configuration
  ♦ Dynamic Host Resolution Protocol (DHCP)
Bootstrapping Problem

- Host doesn’t have an IP address yet
  - So, host doesn’t know what source address to use

- Host doesn’t know who to ask for an IP address
  - So, host doesn’t know what destination address to use

- Solution: shout to discover a server who can help
  - Install a special server on the LAN to answer distress calls

At what layer would an IP address discovery protocol need to run?

A. Link  B. Network  C. Transport  D. Application
DHCP

- Broadcast-based LAN protocol
  - Host broadcasts “DHCP discover” on LAN (e.g. Ethernet broadcast)
  - DHCP server responds with “DHCP offer” message
  - Host requests IP address: “DHCP request” message
  - DHCP server sends address: “DHCP ack” message w/IP address

- Easy to have fewer addresses than hosts (e.g. UCSD wireless) and to renumber network (use new addresses)

- What if host goes away (how to get address back?)
  - Address is a “lease” not a “grant”, has a timeout
  - Host may have different IP addresses at different times?
Private Address Space

- Sometimes you can’t get/don’t want IP addresses
  - An organization wants to change service providers without having to renumber its entire network
  - A network may be unable obtain (or cannot afford) enough IP addresses for all of its hosts

- IP provides private address space anyone can use
  - 10/8, 192.168/16, 172.16.0/20
  - These addresses are not routable—Internet routers should drop packets destined to these so-called bogons

- What good are they if can’t use them on the Internet?
Address Resolution Protocol

- Every node maintains an **ARP table**
  - (IP address, MAC address) pair

- Consult the table when sending a packet
  - Map destination IP address to MAC address
  - Encapsulate the packet and transmit in a frame

- What if the IP address is not in the table?
  - (Link-layer) Broadcast: “Who has IP address x.x.x.x?”
  - Sender caches the result in its ARP table

---

Out which ports does a router send ARP requests?

A. The port a packet came in on  
B. The port a packet will go out on  
C. All ports  
D. All but A
Network Address Translation

- Gateway router can rewrite IP addresses as packets leave or enter a given network
  - I.e., replace private addresses with public ones
  - Router needs to see and update every packet

- Maintains a mapping of private-to-public addresses
  - Simple case is a one-to-one mapping
  - Anytime network changes provider, just update mapping table
  - In more clever scenarios, can map a set of private addresses to a smaller set of public addresses
  - In the extreme map the entire private network to one public IP!
IP Masquerading

- A.K.A. Network Address and port Translation (NAT), Port Address Translation (PAT), or, colloquially, just NAT.
- Entire local network uses just one IP address as far as outside world is concerned:
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).
A NAT’d Network

All packets leaving local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Packets with source or destination in this network have 10.0.0.0/8 address for source, destination (as usual)
**NA(p)T Example**

2: NAT router changes packet source addr from 10.0.0.1:3345 to 138.76.29.7:5001, updates table

<table>
<thead>
<tr>
<th>WAN side addr</th>
<th>LAN side addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>138.76.29.7:5001</td>
<td>10.0.0.4:3345</td>
</tr>
<tr>
<td>……</td>
<td>……</td>
</tr>
</tbody>
</table>

3: Reply arrives dest. address: 138.76.29.7:5001

4: NAT router changes packet dest addr from 138.76.29.7:5001 to 10.0.0.4:3345

1: host 10.0.0.4 sends packet to 132.239.8.45:80
NAT Challenges

- End hosts may not be aware of external IP address
  - Some applications include IP addresses in application data
  - Packets will contain private IP addresses inside payload
  - Many NATs will inspect/rewrite certain protocols, e.g., FTP

- NAT’d end hosts are not reachable from the Internet
  - All connections must be initiated from within private network
  - Alternative is to configure fixed forwarding in NAT
  - Many protocols for **NAT traversal** to get around this
Summary

● Domain Name System
  ◆ Distributed, hierarchical database
  ◆ Distributed collection of servers
  ◆ Caching to improve performance

● IP to MAC Address mapping
  ◆ Dynamic Host Configuration Protocol (DHCP)
  ◆ Address Resolution Protocol (ARP)
For Next Time

- Midterm MONDAY

- Finish up Project 1; due next FRIDAY!