Lecture 12: Naming

CSE 123: Computer Networks
Alex C. Snoeren

HW 2 due FRIDAY
Lecture 12 Overview

- Discovering addresses (DHCP/ARP)
- User-friendly names (DNS)
- Network address translation (NAT)
Layers of Identifiers

- **Link-layer (MAC) address** (e.g., 58:B0:35:F2:3C:D9)
  - Used by *network adaptors* to identify interesting frames
  - Unique, hard-coded identifier “burned into” network adaptor
  - Flat name space (of 48 bits in Ethernet)

- **IP address** (e.g., 128.54.70.238)
  - Used by *routers* to forward packets
  - Unique, topologically meaningful locator
  - Hierarchical namespace of 32 bits

- **Host name** (e.g., www.ucsd.edu)
  - Used by *humans* to specify host of interest
  - Unique, selected by host administrator
  - Hierarchical, variable-length string of alphanumeric characters
**MAC addresses:** 58:B0:35:F2:3C:D9
- **OUIs:** assigned to vendors by the IEEE
- **Adapters:** assigned by the vendor from its block

**IP addresses:** 128.54.70.238
- **Prefixes:** ICANN, regional Internet registries, and ISPs
- **Hosts:** static configuration, or dynamic using DHCP

**Host name:** www.ucsd.edu
- **Domain:** registrar for each top-level domain (e.g., .edu)
- **Host name:** local administrator assigns to each host
Mapping Between Identifiers

- **Address Resolution Protocol (ARP)**
  - Given an IP address, provide the MAC address
  - To enable communication within the Local Area Network

- **Dynamic Host Configuration Protocol (DHCP)**
  - Automates host boot-up process
  - Given a MAC address, assign a unique IP address
  - … and tell host other stuff about the Local Area Network

- **Domain Name System (DNS)**
  - Given a host name, provide the IP address
  - Given an IP address, provide the host name
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
Whence come IP Addresses?

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

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

- You get one 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

```
  host   host   ...   host
  |      |      |      |
  V      V      V      V
  DHCP server
```
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?
Domain Name System (DNS)

- Distributed administrative control
  - Hierarchical name space divided into zones
  - Distributed over a collection of DNS servers

- Hierarchy of DNS servers
  - Root servers
  - Top-level domain (TLD) servers
  - Authoritative DNS servers

- Performing the translations
  - Local DNS servers
  - Resolver software

CSE 123 – Lecture 12: Naming
DNS: Distributed Database

Unnamed root

generic domains

com edu ... org

my.east.bar.edu

CSE 123 – Lecture 12: Naming
DNS Root Servers

- 13 root servers (see http://www.root-servers.org/)
  - Labeled A through M

A Verisign, Dulles, VA
C Cogent, Herndon, VA
D U Maryland College Park, MD
G US DoD Vienna, VA
H ARL Aberdeen, MD
J Verisign (164 locations)

E NASA Mt View, CA
F Internet Sys. C. Palo Alto, CA

K RIPE London
I Netnod, Stockholm
M WIDE Tokyo

B USC-ISI Marina del Rey, CA
L ICANN Los Angeles, CA

CSE 123 – Lecture 12: Naming
Using DNS

- Local DNS server ("default name server")
  - Usually near the end hosts who use it
  - Local hosts configured with local server (e.g., /etc/resolv.conf) or learn the server via DHCP

- Client application
  - Extract server name (e.g., from the URL)
  - Do gethostbyname() to trigger resolver code

- Server application
  - Extract client IP address from socket
  - Optional gethostbyaddr() to translate into name
Example

Host at cis.poly.edu wants IP address for gaia.cs.umass.edu

Requesting host:
cis.poly.edu

Authoritative DNS server:
dns.cs.umass.edu

TLD DNS server:
dns.poly.edu

Root DNS server
Reliability

- DNS servers are replicated
  - Name service available if at least one replica is up
  - Queries can be load balanced between replicas

- UDP used for queries
  - Need reliability: must implement this on top of UDP
  - Try alternate servers on timeout
  - Exponential backoff when retrying same server

- Cache responses to decrease load
  - Both at end hosts and local servers
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?
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!
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).
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

1: host 10.0.0.4 sends packet to 132.239.8.45:80

S: 10.0.0.4:3345
D: 132.239.8.45:80

NAT translation 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

CSE 123 – Lecture 12: Naming
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

- IP to MAC Address mapping
  - Dynamic Host Configuration Protocol (DHCP)
  - Address Resolution Protocol (ARP)

- Domain Name System
  - Distributed, hierarchical database
  - Distributed collection of servers
  - Caching to improve performance
For Next Time

• Homework 2 due at beginning of next class

• Finish up Project 1; due next MONDAY!

• Midterm a week from today