Networking Theory

CSCI 201L

Jeffrey Miller, Ph.D.
jeffrey.miller@usc.edu

HTTP://WWW-SCF.USC.EDU/~CSCI201
Outline

- Networking Overview
  - DNS
  - IP Addressing
  - Subnets
  - DHCP
  - Ports
  - NAT
- Test Yourself
Networking Overview

- A server is a computer that has at least one program running on it that can service requests from another program.
- Server hardware is typically more robust than other hardware, but a server can physically be any computer.
- A client is a computer that requests a service to be performed by another computer.
- Consider browsing the web. What is the service provided by a web server?
DNS

- Some computers can be identified by a hostname and domain name
  - An example would be www.usc.edu
  - www is the hostname (or an alias for a hostname)
  - usc.edu is the domain name

- To find the IP address of a hostname/domain name combination from a command line, run `ping` or `nslookup` from a command line or terminal
The hostname/domain name combination will be mapped to an IP address through DNS servers

- DNS is a hierarchical domain-based naming scheme implemented through a distributed database system for implementing this naming scheme
- DNS was conceived at USC’s ISI and managed there until 1998
- DNS is now managed by ICANN (Internet Corporation for Assigned Names and Numbers)
DNS Resource Records

- Every domain has a set of resource records associated with it, which is what DNS will return based on a certain name.
- A resource record consists of five items:
  - Domain Name – the domain of the record
  - Time To Live – the higher the value, the more stable the record
  - Class – always IN for Internet resources (rarely used outside of that)
  - Type – what kind of record it is (see table below)
  - Value – the value associated with the record

<table>
<thead>
<tr>
<th>Type</th>
<th>Meaning</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOA</td>
<td>Start of Authority</td>
<td>Parameters for this zone</td>
</tr>
<tr>
<td>A</td>
<td>IP address of a host</td>
<td>32-Bit integer</td>
</tr>
<tr>
<td>MX</td>
<td>Mail exchange</td>
<td>Priority, domain willing to accept e-mail</td>
</tr>
<tr>
<td>NS</td>
<td>Name Server</td>
<td>Name of a server for this domain</td>
</tr>
<tr>
<td>CNAME</td>
<td>Canonical name</td>
<td>Domain name</td>
</tr>
<tr>
<td>PTR</td>
<td>Pointer</td>
<td>Alias for an IP address</td>
</tr>
<tr>
<td>HINFO</td>
<td>Host description</td>
<td>CPU and OS in ASCII</td>
</tr>
<tr>
<td>TXT</td>
<td>Text</td>
<td>Uninterpreted ASCII text</td>
</tr>
</tbody>
</table>
### Sample DNS Database

<table>
<thead>
<tr>
<th>Host</th>
<th>Type</th>
<th>Class</th>
<th>TTL</th>
<th>A-Record</th>
<th>MX-Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs.vu.nl</td>
<td>SOA</td>
<td>128</td>
<td>86400</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TXT</td>
<td>128</td>
<td>86400</td>
<td>&quot;Divisie Wiskunde en Informatica.&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TXT</td>
<td>128</td>
<td>86400</td>
<td>&quot;Vrije Universiteit Amsterdam.&quot;</td>
<td></td>
</tr>
<tr>
<td>cs.vu.nl</td>
<td>MX</td>
<td>128</td>
<td>86400</td>
<td>1 zephyr.cs.vu.nl</td>
<td></td>
</tr>
<tr>
<td>cs.vu.nl</td>
<td>MX</td>
<td>128</td>
<td>86400</td>
<td>2 top.cs.vu.nl</td>
<td></td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>HINFO</td>
<td>128</td>
<td>86400</td>
<td>Sun Unix</td>
<td></td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>A</td>
<td>128</td>
<td>86400</td>
<td>130.37.16.112</td>
<td></td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>A</td>
<td>128</td>
<td>86400</td>
<td>192.31.231.165</td>
<td></td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>MX</td>
<td>128</td>
<td>86400</td>
<td>1 flits.cs.vu.nl</td>
<td></td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>MX</td>
<td>128</td>
<td>86400</td>
<td>2 zephyr.cs.vu.nl</td>
<td></td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>MX</td>
<td>128</td>
<td>86400</td>
<td>3 top.cs.vu.nl</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.cs.vu.nl">www.cs.vu.nl</a></td>
<td>CNAME</td>
<td>128</td>
<td>86400</td>
<td>star.cs.vu.nl</td>
<td></td>
</tr>
<tr>
<td>ftp.cs.vu.nl</td>
<td>CNAME</td>
<td>128</td>
<td>86400</td>
<td>zephyr.cs.vu.nl</td>
<td></td>
</tr>
<tr>
<td>rowboat</td>
<td>A</td>
<td>128</td>
<td>86400</td>
<td>130.37.56.201</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MX</td>
<td>128</td>
<td>86400</td>
<td>1 rowboat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MX</td>
<td>128</td>
<td>86400</td>
<td>2 zephyr</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HINFO</td>
<td>128</td>
<td>86400</td>
<td>Sun Unix</td>
<td></td>
</tr>
<tr>
<td>little-sister</td>
<td>A</td>
<td>128</td>
<td>86400</td>
<td>130.37.62.23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HINFO</td>
<td>128</td>
<td>86400</td>
<td>Mac MacOS</td>
<td></td>
</tr>
<tr>
<td>laserjet</td>
<td>A</td>
<td>128</td>
<td>86400</td>
<td>192.31.231.216</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HINFO</td>
<td>128</td>
<td>86400</td>
<td>&quot;HP Laserjet IIISi&quot; Proprietary</td>
<td></td>
</tr>
</tbody>
</table>
Actual DNS Records

Zone File Editor

Filter
- A Record (Host)
- CNAME (Alias)
- MX (Mail Exchanger)
- TXT (Text)
- SRV (Service)
- AAAA (IPv6 Host)
- NS (Nameserver)

Answer Center

Networking Overview - DNS
IP Addresses

- An IP address is a unique address that is required of all computers that communicate on a network.
- IP addresses are broken into a network address and a host address.
- IPv4 addresses consist of 32 bits separated as 4 numbers of 8 bits each.
  - 128.125.253.146
- The IPv4 network and host addresses are determined by the class of the IP address (see next slide).
- IPv6 addresses consist of 128 bits separated as 8 sets of 4 hexadecimal values.
  - NOTE that if all four hexadecimal values are 0, the term will be omitted.
    - fe29:392A:3396::5591:40d3 (4th, 7th, and 8th terms are 0000)
IPv4 Classes

- Network numbers are managed by ICANN
# IPv4 Special Addresses

<table>
<thead>
<tr>
<th></th>
<th>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</th>
<th>This host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>0 0 ... 0 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</td>
<td>Broadcast on the local network</td>
</tr>
<tr>
<td>Network</td>
<td>1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</td>
<td>Broadcast on a distant network</td>
</tr>
<tr>
<td>127</td>
<td>(Anything)</td>
<td>Loopback</td>
</tr>
</tbody>
</table>
Public and Private IP Addresses

- Public IP addresses are able to be seen by any computer in the world and are required for communicating on the Internet.
- Private IP addresses are typically secured behind a firewall, so explicit access has to be allowed to them.
  - Private IPv4 addresses are in the following ranges:
    - Class A Private: 10.0.0.0 – 10.255.255.255
      - 2^0=1 network with 2^24 addresses
    - Class B Private: 172.16.0.0 – 172.31.255.255
      - 2^4=16 networks with 2^16 addresses
    - Class C Private: 192.168.0.0 – 192.168.255.255
      - 2^8=256 networks with 2^8 hosts on each network
  - Private IP addresses must use NAT if accessing the Internet because private IP addresses cannot communicate on the Internet.
    - NAT is discussed on later slide.
  - If a computer is unable to obtain an IP address, an address in the range 169.254.0.0 – 169.254.255.255 may be assigned.
    - This IP address is NOT available to the Internet.
Finding Your IP Address

- Open a command line and type `ipconfig` in Windows or `ifconfig` in Mac or Linux.
IPv4 Header

- **Version** – which version of IP is being used (though there is a different header for IPv6)
- **IHL (Internet Header Length)** – tells how long the header is, in 32-bit words. The minimum value is 5, maximum is 15 (limiting the header to 60 bytes)
- **Type of Service** – intended to distinguish between different classes of service, such as reliability and speed, though most routers ignore this field
- **Total Length** – maximum length is 65535 bytes
- **Identification** – all fragments of a datagram contain the same Identification value
- **DF – Don’t Fragment**
- **MF – More Fragments**, used to know when the last fragment of a datagram has arrived
- **Fragment Offset** – where in the current datagram this fragment belongs
- **Time to Live (TTL)** – counter used to limit packet lifetimes based on number of hops, decremented on each hop
- **Protocol** – protocol used in data portion of the IP packet, such as IPv4, tunneled, encapsulated, MANET, exterior gateway protocol, etc.
- **Header Checksum** – verifies the header only and must be recomputed at each hop since the TTL changes
- **Options** – are not used by all routers, so are irrelevant
IPv6 Header

- Version – which version of IP is being used (constant value 0110)
- Traffic Class – differentiated services (6 bits) and explicit congestion notification (2 bits)
  - Quality of service
  - End-to-end notification of network congestion without dropping packets
- Flow Label – tells routers that packets with same label should stay on the same path
- Payload Length – size of payload in octets
- Next Header – specifies the type of the next header
- Hop Limit – replaces the time to live field in IPv4
- Source Address – IPv6 address of sending node
- Destination Address – IPv6 address of destination node
Subnets

- Since network addresses are so scarce, we can take a few bits away from the host address to make a subnet within a network.

- To implement subnetting, the router needs a subnet mask that indicates the split between the network and the subnet/host combination.

- The subnet mask will consist of all 1’s followed by all 0’s.
  - \[255.255.255.0 = 11111111 \ 11111111 \ 11111111 \ 00000000\] Valid
  - \[255.255.255.2 = 11111111 \ 11111111 \ 11111111 \ 00000010\] Not valid

- The subnet mask can also be written using slash notation.
  - The number after the slash will represent the number of bits to be used in the subnet address.
  - This would correspond to the number of 1’s in the subnet mask.
Subnets

- Assume a host has an IP address of 74.125.127.104 with a subnet mask of 255.255.255.192 (also written as 74.125.127.104/26)
  - What is the network address? (i.e. what class IP address is this?)
  - What is the subnet mask in binary?
  - How many hosts can be in the subnet?

- Network Address – this is a Class A address, so the first 8 bits are allocated for the network: 74.0.0.0
- Subnet Mask in binary will have the first 26 bits as 1’s with the last 6 bits as 0’s
- # Hosts – the last 6 bits are reserved for hosts, giving $2^6=64$ host addresses for this subnet
To get the network/subnet address from an IP address and subnet mask, perform a logical AND operation between them.

\[
\begin{align*}
137.229.154.221 &= 1000\ 1001\ 1110\ 0101\ 1001\ 1010\ 1101\ 1101 \\
255.255.224.0 &= 1111\ 1111\ 1111\ 1111\ 1110\ 0000\ 0000\ 0000 \\
137.229.128.0 &= 1000\ 1001\ 1110\ 0101\ 1000\ 0000\ 0000\ 0000
\end{align*}
\]

The subnet address is 137.229.128.0

This subnet mask provides 19 bits for the network address and 13 bits for the host address.

Another way we could have written the IP address with the subnet mask is 137.229.154.221/19.

Note that the subnet mask can never contain fewer bits than the number of bits in the network address.

Why does that make sense?
DHCP

- Dynamic Host Control Protocol (DHCP) is used for a computer or router to automatically assign IP addresses and other network configuration (such as the gateway and subnet mask) to computers on the network.
  - These addresses can be private or public IP addresses.
  - Most routers assign private IP addresses, such as 192.168.1.101.
  - Routers often have DHCP servers built into them.
Ports

- Since more than one networked program can run on a computer at the same time, we need a way to uniquely identify them
  - Ports allow us to do just that
- A port is typically in the range from 0 to 65535 (16 bits)
  - Ports from 0-1023 (inclusively) are reserved for well-known applications, so root or administrator access is required to run a program on a port in that range
  - Ports from 1024-49151 (inclusively) are registered ports and can be used by any application
  - Ports from 49152-65535 are dynamic or private ports and are typically used by the operating system when an application needs to pass an application off to a non-registered port
Well-Known Ports

- 20 FTP data
- 21 FTP control
- 22 SSH
- 23 Telnet
- 25 SMTP
- 53 DNS
- 80 HTTP
- 143 IMAP
- 443 HTTPS

There are many others, but these are some of the more popular ones.
Network Address Translation (or IP Masquerading) allows a computer to have a private IP address:

- Private IP addresses are not able to be accessed by hosts outside of the local network.
- A NAT server (usually implemented in a router) substitutes its own public IP address in place of the computer’s private IP address.
- The NAT server must maintain a NAT table that links the private IP address and TCP/UDP source port combination to the destination IP address.
  - Since the NAT server’s public IP address has been substituted for the computer’s private IP address in the packet, the response from the destination computer will come back to the NAT server.
  - The port will let the NAT server know to which computer to forward the response.
Outline

- Networking Overview
  - DNS
  - IP Addressing
  - Subnets
  - DHCP
  - Ports
  - NAT
- Test Yourself
Test Yourself

- For each of the following IP addresses and subnets, write out the IP address in binary, subnet address in decimal, subnet address in binary, and the range of IP addresses that can be assigned to hosts.
  - 65.145.211.3/15
  - 145.21.48.129/25
  - 211.14.68.244/29

- Explain why the following IP address/subnet combination does not make sense.
  - 225.14.25.124/22

- Why are ports needed for NAT?