CMPE 150 -- Introduction to Computer Networks

- Instructor: Patrick Mantey
  mantey@soe.ucsc.edu
  http://www.soe.ucsc.edu/~mantey/
- Office: Engr. 2 Room 595J
- Office hours: Tues 3-5 PM, Mon 5-6 PM*
- TA: Anselm Kia
  akia@soe.ucsc.edu
- Web site: http://www.soe.ucsc.edu/classes/cmpe150/Winter09/
- Text: Tannenbaum: Computer Networks
  (4th edition – available in bookstore, etc.)
# Syllabus

<table>
<thead>
<tr>
<th>Lecture</th>
<th>Date</th>
<th>Topic</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6-Jan</td>
<td>Intro / Overview</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>2</td>
<td>8-Jan</td>
<td>Internet Architecture</td>
<td>Chapter 1, 2</td>
</tr>
<tr>
<td>3</td>
<td>13-Jan</td>
<td>Physical Layer</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>4</td>
<td>15-Jan</td>
<td>Physical Layer</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>5</td>
<td>20-Jan</td>
<td>Link Layer</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>6</td>
<td>22-Jan</td>
<td>Link Layer / MAC</td>
<td>Chapter 3, 4</td>
</tr>
<tr>
<td>7</td>
<td>27-Jan</td>
<td>MAC Sublayer</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>8</td>
<td>29-Jan</td>
<td>Wireless</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>9</td>
<td>3-Feb</td>
<td>Bridges (and Review)</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>10</td>
<td>5-Feb</td>
<td><strong>Midterm Exam 1</strong></td>
<td>Chapter 4</td>
</tr>
<tr>
<td>11</td>
<td>10-Feb</td>
<td>Intro to Network Layer</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>12</td>
<td>12-Feb</td>
<td>Routing and Routers</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>13</td>
<td>17-Feb</td>
<td>Congestion Control, QOS</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>14</td>
<td>19-Feb</td>
<td>Internet Networking / IP</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>15</td>
<td>24-Feb</td>
<td>Transport Layer / Services/ Protocols</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>16</td>
<td>26-Feb</td>
<td>Internet Transport Protocols: UDP, TCP</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>17</td>
<td>3-Mar</td>
<td>RPC/ TCP/ Performance / Applications / Review</td>
<td>Chapter 6, 7</td>
</tr>
<tr>
<td>18</td>
<td>5-Mar</td>
<td><strong>Midterm Exam 2</strong></td>
<td>Chapter 7</td>
</tr>
<tr>
<td>19</td>
<td>10-Mar</td>
<td>Applications / Multimedia</td>
<td>Chapter 7</td>
</tr>
<tr>
<td>20</td>
<td>12-Mar</td>
<td>Buffer / Review</td>
<td>Chapter 7</td>
</tr>
<tr>
<td><strong>Final Exam</strong></td>
<td>18-Mar</td>
<td>12-3 PM</td>
<td></td>
</tr>
</tbody>
</table>
Today’s Agenda

- Network Layer
  - Quality of Service
  - Internetworking
  - IP
Text Readings

Today:
- Chapter 5, section 5.4, 5.5, 5.6: *Internet Protocol*

Tuesday:
- Chapter 6: Transport Layer
Problem Assignment #5

- On class web page this afternoon
- Due Tuesday, February 24
Internet Layering

Level 5  -- **Application** Layer  
            (rlogin, ftp, SMTP, POP3, IMAP, HTTP..)

Level 4  -- **Transport** Layer (a.k.a Host-to-Host)  
            *(TCP, UDP)*

Level 3  -- **Network** Layer (a.k.a. Internet)  
            *(IP, ICMP, ARP)*

Level 2  -- *(Data) **Link*** Layer / MAC sub-layer  
            (a.k.a. Network Interface or Network Access Layer)

Level 1  -- **Physical** Layer
Leaky and Token Bucket Algorithms

(a) Input to a leaky bucket. (b) Output from a leaky bucket. Output from a token bucket with capacities of (c) 250 KB, (d) 500 KB, (e) 750 KB, (f) Output from a 500KB token bucket feeding a 10-MB/sec leaky bucket.
Flow Specifications

• Way for user/application to specify traffic patterns and desired quality of service.
  – Before connection is established or data is sent, source provides flow spec to network.
  – Network can accept, reject, or counter-offer.
  – Traffic spec: maximum packet size, maximum transmission rate.
  – Service desired: maximum acceptable loss rate, maximum delay and delay variation.
Admission Control

Examples of flow specification

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token bucket rate</td>
<td>Bytes/sec</td>
</tr>
<tr>
<td>Token bucket size</td>
<td>Bytes</td>
</tr>
<tr>
<td>Peak data rate</td>
<td>Bytes/sec</td>
</tr>
<tr>
<td>Minimum packet size</td>
<td>Bytes</td>
</tr>
<tr>
<td>Maximum packet size</td>
<td>Bytes</td>
</tr>
</tbody>
</table>
Packet Scheduling

(a) A router with five packets queued for line O.

(b) Finishing times for the five packets.

Packets send in the order of their finishing – “fair queueing” byte-by-byte – equal priority
Flow-Based Algorithms

• Used for multimedia
• New about 1995-7
• RSVP – RFC 2205
  – Multicast routing
  – Spanning trees
  – Group address carried in the packet
  – All receivers can send reservation request to sender
RSVP-The ReSerVation Protocol

(a) A network,  (b) The multicast spanning tree for host 1.  
(c) The multicast spanning tree for host 2.
RSVP-The ReSerVation Protocol (2)

(a) Host 3 requests a channel to host 1. (b) Host 3 then requests a second channel, to host 2. (c) Host 5 requests a channel to host 1.
Differentiated Services

• Problems with Flow-base Algorithms
  – Advance setup required
  – Flow depends on routers not crashing
  – Complex router-to-router exchanges for setup
  – So RSVP rarely used!

• Differentiated Services
  – Limited to an “administrative domain”
  – *Class-based* *(vs. flow-based)* service
Differentiated Service where “Expedited” packets experience a traffic-free network.
Assured Forwarding

A possible implementation of the data flow for assured forwarding.
Frame Format for Label Switching and MPLS

Transmitting a TCP segment using IP, MPLS (multiprotocol label switching), and PPP.
Internetworking

- How Networks Differ
- How Networks Can Be Connected
- Concatenated Virtual Circuits
- Connectionless Internetworking
- Tunneling
- Internetwork Routing
- Fragmentation
Connecting Networks

A collection of interconnected networks.
### How Networks Differ

<table>
<thead>
<tr>
<th>Item</th>
<th>Some Possibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service offered</td>
<td>Connection oriented versus connectionless</td>
</tr>
<tr>
<td>Protocols</td>
<td>IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.</td>
</tr>
<tr>
<td>Addressing</td>
<td>Flat (802) versus hierarchical (IP)</td>
</tr>
<tr>
<td>Multicasting</td>
<td>Present or absent (also broadcasting)</td>
</tr>
<tr>
<td>Packet size</td>
<td>Every network has its own maximum</td>
</tr>
<tr>
<td>Quality of service</td>
<td>Present or absent; many different kinds</td>
</tr>
<tr>
<td>Error handling</td>
<td>Reliable, ordered, and unordered delivery</td>
</tr>
<tr>
<td>Flow control</td>
<td>Sliding window, rate control, other, or none</td>
</tr>
<tr>
<td>Congestion control</td>
<td>Leaky bucket, token bucket, RED, choke packets, etc.</td>
</tr>
<tr>
<td>Security</td>
<td>Privacy rules, encryption, etc.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Different timeouts, flow specifications, etc.</td>
</tr>
<tr>
<td>Accounting</td>
<td>By connect time, by packet, by byte, or not at all</td>
</tr>
</tbody>
</table>

Some of the many ways networks can differ.
How Networks Can Be Connected

(a) Two Ethernets connected by a switch.
(b) Two Ethernets connected by routers

*Multiprotocol routers* is networks differ
Concatenated Virtual Circuits

Internetworking using concatenated virtual circuits.
Connectionless Internetworking

- Packets travel individually and can take different routes.
Tunneling

Tunneling a packet from Paris to London
-- with source and destination same type of network.
Tunneling (2)

Tunneling a car from France to England.
Internetwork Routing 1

• 2-level hierarchy:
  – Routing within each network: interior gateway protocol.
  – Routing between networks: exterior gateway protocol.

• Within each network, different routing algorithms can be used.

• Each network is autonomously managed and independent of others: autonomous system (AS).
Internetwork Routing 2

• Typically, packet starts in its LAN. Gateway receives it (broadcast on LAN to “unknown” destination).

• Gateway sends packet to gateway on the destination network using its routing table. If it can use the packet’s native protocol, sends packet directly. Otherwise, tunnels it.
Internetwork Routing

(a) An internetwork.  (b) A graph of the internetwork.
Fragmentation 1

• Network-specific maximum packet size.
  – Width of TDM slot.
  – OS buffer limitations.
  – Protocol (number of bits in packet length field).

• Maximum payloads range from 48 bytes (ATM cells) to 64Kbytes (IP packets).
Fragmentation 2

• What happens when large packet wants to travel through network with smaller maximum packet size? *Fragmentation.*

• Gateways break packets into *fragments*; each sent as separate packet.

• Gateway on the other side have to reassemble fragments into original packet.

• 2 kinds of fragmentation: transparent and non-transparent.
Fragmentation

(a) Transparent fragmentation.
(b) Nontransparent fragmentation.
• Fragmentation when the elementary data size is 1 byte.
• (a) Original packet, containing 10 data bytes.
• (b) Fragments after passing through a network with maximum packet size of 8 payload bytes plus header.
• (c) Fragments after passing through a size 5 gateway.
Transparent Fragmentation

• Small-packet network transparent to other subsequent networks.

• Fragments of a packet addressed to the same exit gateway, where packet is reassembled.
  – OK for concatenated VC internetworking.

• Subsequent networks are not aware fragmentation occurred.

• ATM networks (through special hardware) provide transparent fragmentation: segmentation.
Problems with Transparent Fragmentation

• Exit gateway must know when it received all the pieces.
  - Fragment counter or “end of packet” bit.
• Some performance penalty but requiring all fragments to go through same gateway.
• May have to repeatedly fragment and reassemble through series of small-packet networks.
Non-Transparent Fragmentation

• Only reassemble at destination host.
  – Each fragment becomes a separate packet.
  – Thus routed independently.

• Problems:
  – Hosts must reassemble.
  – Every fragment must carry header until it reaches destination host.
Keeping Track of Fragments 1

• Fragments must be numbered so that original data stream can be reconstructed.

• Tree-structured numbering scheme:
  – Packet 0 generates fragments 0.0, 0.1, 0.2, ...
  – If these fragments need to be fragmented later on, then 0.0.0, 0.0.1, ..., 0.1.0, 0.1.1, ...
  – But, too much overhead in terms of number of fields needed.
  – Also, if fragments are lost, retransmissions can take alternate routes and get fragmented differently.
Keeping Track of Fragments 2

• Another way is to define elementary fragment size that can pass through every network.
• When packet fragmented, all pieces equal to elementary fragment size, except last one (may be smaller).
• Packet may contain several fragments.
Keeping Track of Fragments 3

- Header contains packet number, number of first fragment in the packet, and last-fragment bit.

(a) Original packet with 10 data bytes.

(b) Fragments after passing through network with maximum packet size = 8 bytes.
The Network Layer in the Internet

- The IP Protocol
- IP Addresses
- Internet Control Protocols
- OSPF – The Interior Gateway Routing Protocol
- BGP – The Exterior Gateway Routing Protocol
- Internet Multicasting
- Mobile IP
- IPv6
Design Principles for Internet

• Make sure it works.
• Keep it simple.
• Make clear choices.
• Exploit modularity.
• Expect heterogeneity.
• Avoid static options and parameters.
• Look for a good design; it need not be perfect.
• Be strict when sending and tolerant when receiving.
• Think about scalability.
• Consider performance and cost.
Collection of Subnetworks

The Internet is an interconnected collection of networks.
IP (Internet Protocol)

- Glues Internet together.
- Common network-layer protocol spoken by all Internet participating networks.
- Best effort datagram service:
  - No reliability guarantees.
  - No ordering guarantees.
IP

• Transport layer breaks data streams into datagrams; fragments transmitted over Internet, possibly being fragmented.

• When all packet fragments arrive at destination, reassembled by network layer and delivered to transport layer at destination host.
IP Versions

• IPv4: IP version 4.
  – Current, predominant version.
  – 32-bit long addresses.

• IPv6: IP version 6 (aka, IPng).
  – Longer addresses (16-byte long).
IP Datagram Format

• IP datagram consists of header and data (or payload).

• Header:
  – 20-byte fixed (mandatory) part.
  – Variable length optional part.
The IP Protocol

The IPv4 (Internet Protocol) header.

<table>
<thead>
<tr>
<th>Version</th>
<th>IHL</th>
<th>Type of service</th>
<th>Total length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Identification</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time to live</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Options (0 or more words)</td>
<td></td>
</tr>
</tbody>
</table>
The IP Protocol (2)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Specifies how secret the datagram is</td>
</tr>
<tr>
<td>Strict source routing</td>
<td>Gives the complete path to be followed</td>
</tr>
<tr>
<td>Loose source routing</td>
<td>Gives a list of routers not to be missed</td>
</tr>
<tr>
<td>Record route</td>
<td>Makes each router append its IP address</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Makes each router append its address and timestamp</td>
</tr>
</tbody>
</table>

- Some of the IP options.
IP Address Formats

32 Bits

<table>
<thead>
<tr>
<th>Class</th>
<th>Network</th>
<th>Host</th>
<th>Range of host addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td></td>
<td>1.0.0.0 to 127.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>10</td>
<td></td>
<td>128.0.0.0 to 191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>110</td>
<td></td>
<td>192.0.0.0 to 223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td>1110</td>
<td>Multicast address</td>
<td>224.0.0.0 to 239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td>1111</td>
<td>Reserved for future use</td>
<td>240.0.0.0 to 255.255.255.255</td>
</tr>
</tbody>
</table>
### Special IP Addresses

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 0</td>
<td>...</td>
<td>0 0</td>
<td></td>
<td></td>
<td>Host</td>
</tr>
<tr>
<td></td>
<td>1 1 1 1 1</td>
<td>1 1 1 1 1</td>
<td>1 1 1 1 1</td>
<td>1 1 1 1 1</td>
<td>1 1 1 1 1</td>
<td>1 1 1 1 1</td>
</tr>
<tr>
<td></td>
<td>Network</td>
<td>1 1 1 1</td>
<td>...</td>
<td>1 1 1 1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>127</td>
<td></td>
<td>(Anything)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **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** This host
- **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** A host on this network
- **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** Broadcast on the local network
- **Network 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** Broadcast on a distant network
- **127 (Anything)** Loopback
A campus network consisting of LANs for various departments.
A class B network subnetted into 64 subnets.
CIDR – Classless InterDomain Routing

<table>
<thead>
<tr>
<th>University</th>
<th>First address</th>
<th>Last address</th>
<th>How many</th>
<th>Written as</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cambridge</td>
<td>194.24.0.0</td>
<td>194.24.7.255</td>
<td>2048</td>
<td>194.24.0.0/21</td>
</tr>
<tr>
<td>Edinburgh</td>
<td>194.24.8.0</td>
<td>194.24.11.255</td>
<td>1024</td>
<td>194.24.8.0/22</td>
</tr>
<tr>
<td>Oxford</td>
<td>194.24.16.0</td>
<td>194.24.31.255</td>
<td>4096</td>
<td>194.24.16.0/20</td>
</tr>
</tbody>
</table>

A set of IP address assignments.
NAT – Network Address Translation

Placement and operation of a NAT box.
Firewalls 1

• Analogy: ditch around medieval castles.
  – To enter or exit castle, must pass over single bridge.

• Firewalls force traffic to and from company through single point.

• Firewalls typically consist of:
  – Packet filters (one for incoming, other for outgoing packets).
  – Application gateway.
Firewalls 2

- Packet filter: router equipped with capability of inspecting packets.
  - Packets that meet criteria are forwarded; others discarded.
- Application gateways operate at application level; e.g., mail gateway.
Network Probing

**ping traceroute** *(tracert in Windows)*

**Nslookup**  http://www.zoneedit.com/lookup.html

Network Monitor (UCSC)
http://noc.ucsc.edu/

Bandwith tester: http://nitro.ucsc.edu/


http://www.analysespider.com/ip2country/lookup.php


http://cities.lk.net/traceroute.htm

http://www.caida.org/tools/utilities/others/pathchar/

http://visualroute.visualware.com/
(try dit.upm.es 138.4.2.61 or 137.132.90.6)
over a maximum of 30 hops:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Time1</th>
<th>Time2</th>
<th>Time3</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 ms</td>
<td>1 ms</td>
<td>1 ms</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>2</td>
<td>24 ms</td>
<td>23 ms</td>
<td>23 ms</td>
<td>L100.DSL-01.SNFCCA.verizon-gni.net [71.116.64.1]</td>
</tr>
<tr>
<td>3</td>
<td>31 ms</td>
<td>40 ms</td>
<td>44 ms</td>
<td>at-4-3-0-1711.CORE-RTR2.SJC01.verizon-gni.net [130.81.135.32]</td>
</tr>
<tr>
<td>4</td>
<td>73 ms</td>
<td>73 ms</td>
<td>60 ms</td>
<td>so-0-3-0-0.SJC01-BB-RTR2.verizon-gni.net [130.81.20.46]</td>
</tr>
<tr>
<td>5</td>
<td>25 ms</td>
<td>28 ms</td>
<td>29 ms</td>
<td>0.so-5-3-0.XL4.SJC7.ALTER.NET [152.63.1.161]</td>
</tr>
<tr>
<td>6</td>
<td>45 ms</td>
<td>65 ms</td>
<td>44 ms</td>
<td>0.so-0-3-0.XT2.SCL2.ALTER.NET [152.63.48.1]</td>
</tr>
<tr>
<td>7</td>
<td>59 ms</td>
<td>62 ms</td>
<td>65 ms</td>
<td>sjp-brdr-01.inet.qwest.net [63.146.26.201]</td>
</tr>
<tr>
<td>8</td>
<td>48 ms</td>
<td>28 ms</td>
<td>28 ms</td>
<td>snj-core-01.inet.qwest.net [205.171.233.21]</td>
</tr>
<tr>
<td>9</td>
<td>36 ms</td>
<td>36 ms</td>
<td>33 ms</td>
<td>los-core-01.inet.qwest.net [67.14.22.34]</td>
</tr>
<tr>
<td>10</td>
<td>34 ms</td>
<td>35 ms</td>
<td>43 ms</td>
<td>los-edge-01.inet.qwest.net [205.171.32.34]</td>
</tr>
<tr>
<td>11</td>
<td>35 ms</td>
<td>36 ms</td>
<td>34 ms</td>
<td>63.147.28.182</td>
</tr>
<tr>
<td>12</td>
<td>34 ms</td>
<td>34 ms</td>
<td>35 ms</td>
<td>dc-svl-isp--lax-isp-t2.cenic.net [137.164.40.222]</td>
</tr>
<tr>
<td>13</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Request timed out.</td>
</tr>
<tr>
<td>14</td>
<td>44 ms</td>
<td>44 ms</td>
<td>45 ms</td>
<td>isb-g-GE2-4.ucsc.edu [128.114.0.42]</td>
</tr>
<tr>
<td>15</td>
<td>46 ms</td>
<td>44 ms</td>
<td>46 ms</td>
<td>e2-g-GE1-2.ucsc.edu [128.114.0.78]</td>
</tr>
<tr>
<td>16</td>
<td>44 ms</td>
<td>44 ms</td>
<td>44 ms</td>
<td>tanzanite.cse.ucsc.edu [128.114.56.133]</td>
</tr>
</tbody>
</table>

Trace complete.