CMPE 150 – Winter 2009

Lecture 14

February 24, 2009

P.E. Mantey
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 5</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>Interneting / 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>Final Exam</td>
<td>18-Mar</td>
<td>12-3 PM</td>
<td></td>
</tr>
</tbody>
</table>
Today’s Agenda

- Network Layer
  - IP – ICMP
  - ARP, RARP, BOOTP, DHCP
  - Internet Routing
    - EGP
    - IGP
  - IP Multicasting
  - IPv6

- Intro to Transport Layer
Text Readings

Today:
- Chapter 6: Transport Layer
  - Sections 6.1-6.2.3

Thursday
- Chapter 6, Sections 6.2.4-6, 6.3-6.5 (TCP)
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
NAT – Network Address Translation

Placement and operation of a NAT box.
Internet Control Message Protocol

<table>
<thead>
<tr>
<th>Message type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination unreachable</td>
<td>Packet could not be delivered</td>
</tr>
<tr>
<td>Time exceeded</td>
<td>Time to live field hit 0</td>
</tr>
<tr>
<td>Parameter problem</td>
<td>Invalid header field</td>
</tr>
<tr>
<td>Source quench</td>
<td>Choke packet</td>
</tr>
<tr>
<td>Redirect</td>
<td>Teach a router about geography</td>
</tr>
<tr>
<td>Echo request</td>
<td>Ask a machine if it is alive</td>
</tr>
<tr>
<td>Echo reply</td>
<td>Yes, I am alive</td>
</tr>
<tr>
<td>Timestamp request</td>
<td>Same as Echo request, but with timestamp</td>
</tr>
<tr>
<td>Timestamp reply</td>
<td>Same as Echo reply, but with timestamp</td>
</tr>
</tbody>
</table>

The principal ICMP message types.
Mapping IP to DLL Address

• Internet applications refer to hosts by their IP addresses; once packet gets to destination LAN, node needs to figure out the destination DLL address.

• One solution is to have configuration file.
  – Hard to maintain/update.

• Address Resolution Protocol (ARP):
  – Run by every node to map IP to DLL address (RFC 826).
ARP and DHCP

- What is the Ethernet address for this packet?
  - Solved by Address Resolution Protocol (ARP)
- What is the IP address for this MAC address?
- Give me an IP address (now that I am connected).
- Reverse Address Resolution Protocol:
  - broadcast and hope (RARP sever) knows your machine
    (broadcast restricted to your LAN)

- BOOTP: Like RARP, but uses UDP messages that get forwarded by routers (ARP requests are not forwarded)
  - allows more centralized table
  - requires manual configuration of tables (admin problem)

- Dynamic Host Configuration Protocol – extension of BOOTP
ARP – The Address Resolution Protocol

Three interconnected /24 networks: two Ethernets and an FDDI ring.
ARP

- IP layer builds an Ethernet frame containing IP address whose MAC address is sought
- This frame is broadcast on the LAN
- This frame is not forwarded to other LANs
- The station with owning the IP address sent responds with its MAC address in a response frame
- Sender caches responses (with TTL)
ARP

• Advantage:
  – Easy to administer, less human intervention.
  – Example: 2 hosts on the same Ethernet want to communicate.
    • Host 1 must figure out host 2’s Ethernet address.
    • Host 1 broadcasts ARP packet on Ethernet asking for the Ethernet address of host 2.
    • Host 2 receives the ARP request, and replies with its Ethernet address.
ARP Optimizations

• Caching of ARP replies.
  – Entries may have large TTLs.

• When sending ARP request, piggyback its own IP-DLL address mapping.

• Every machine broadcasts its mapping at boot time.
  – No response is expected.
  – Other machines cache that information.
Proxy ARP

- What if host 1 wants to send data to host 3 on a different LAN?
  - Router connecting the 2 LANs can be configured to respond to ARP requests for the networks it interconnects: proxy arp.
  - Another solution is for host 1 to recognize host 3 is on remote network and use default LAN address that handles all remote traffic; that could be the router’s Ethernet address.
RARP

- Reverse Address Resolution Protocol.
- Given LAN address, what’s the IP address?
- Usually for booting diskless workstation.
  - Gets the OS image from remote file server.
  - Same image for all machines.
  - Machine broadcasts its LAN address.
  - Remote RARP server responds with machine’s IP address.
BOOTP

• RARP broadcasts are not forwarded by routers.
• Need RARP server on every network.
• BOOTP uses UDP messages that are forwarded by routers.
  – Also provides additional information such as IP address of file server holding OS image, subnet mask, etc.
DHCP

- Allow manual and automatic assignment of IP address
- Special server gives out IP addresses
- Need not be on your LAN
- Uses DHCP relay agent on each LAN to get to server
- Machine (after booting) broadcasts DHCP discover packet
- Relay agent sends to DHCP server
- “Lease” of IP address makes them reusable
  - Renew your lease or lose the address
Dynamic Host Configuration Protocol

Operation of DHCP.

Newly-booted host looking for its IP address

DHCP Discover packet (broadcast)

DHCP relay

Other networks

Router

Unicast packet from DHCP relay to DHCP server

DHCP server
Internet Routing

• IGPs and EGPs
  – IGPs: routing within ASs. (Autonomous Systems)
  – EGPs: routing between ASs.
Interior Gateway Protocols (IGP)

- Original Internet IGP was RIP.
  - Distance vector.
  - OK for small ASs but not efficient as ASs got larger.

- New IGP: OSPF.
  - Open Shortest Path First (OSPF).
  - Became standard in 1990.
  - Link state algorithm.
  - RIP is still running but OSPF is taking over.
OSPF – The Interior Gateway Routing Protocol

(a) An autonomous system.
(b) A graph representation of (a).
OSPF (2)

- The relation between ASes, backbones, and areas in OSPF.
OSPF (3)

- The five types of OSPF messages.

<table>
<thead>
<tr>
<th>Message type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>Used to discover who the neighbors are</td>
</tr>
<tr>
<td>Link state update</td>
<td>Provides the sender’s costs to its neighbors</td>
</tr>
<tr>
<td>Link state ack</td>
<td>Acknowledges link state update</td>
</tr>
<tr>
<td>Database description</td>
<td>Announces which updates the sender has</td>
</tr>
<tr>
<td>Link state request</td>
<td>Requests information from the partner</td>
</tr>
</tbody>
</table>
OSPF (4)

• Design requirements:
  – Open implementation.
  – Support for various distance metrics: delay, hops, etc.
  – Dynamic: automatically adapt to topology changes.
  – QoS Routing: real-time versus other traffic using IP’s type of service field.
  – Load balancing across multiple lines.
  – Security and tunneling.
OSP (5)

• Abstracts collection of networks, routers and lines into a directed graph where edges are assigned a cost proportional to the routing metric.
• It then computes shortest path.
• Hierarchical routing within ASs.
  – Areas: collection of contiguous networks.
  – Area 0: AS backbone; all areas connected to it.
OSPF (6)

• Type of service routing:
  – Uses different graphs labeled with different metrics.

• Routing updates:
  – *Adjacent routers* exchange routing information.
  – Adjacent routers are on different LANs.
  – Reliable link state updates with sequence #’s.
Exterior Gateway Protocols (EGPs)

- Routing protocol between ASs.
- Take policy into account.
  - An AS may not be willing to carry traffic originating and destined to foreign ASs.
  - Example: phone companies are willing to carry traffic for their customers but not for others.
Routing Policy Examples

• No transit traffic through certain ASs.
• Traffic source restricts ASs through which its traffic crosses.
• Same for destination.
BGP – The Exterior Gateway Routing Protocol

- (a) A set of BGP routers.

(b) Information sent to F.

Information F receives from its neighbors about D:

From B: "I use BCD"
From G: "I use GCD"
From I: "I use IFGCD"
From E: "I use EFGCD"
BGP (2)

- Border Gateway Protocol.
- THE Exterior Gateway Routing Protocol
- Policies are manually configured into BGP routers.
- BGP abstracts networks as a collection of BGP routers and their links.
- 2 BGP routers are connected if they share a common network.
- BGP routers communicate reliably using TCP.
BGP (3)

• 3 types of networks:
  – Stub networks: have a single connection in the BGP graph; cannot carry transit traffic.
  – Multi-connected networks: have multiple connections but refuse to carry transit traffic.
  – Transit networks: agree to carry transit (3rd. party) traffic possibly with some restriction; e.g., backbones.
BGP (4)

• BGP is a distance vector protocol.
• Routing table entries keep whole path to destination + distance.
• BGP routers can discard the paths containing itself: avoiding loops and counting to infinity.
• Routers compute distance associated to a route taking policy into account.
  – If policy is violated, distance = infinity.
Internet Multicasting

• IP supports multicasting using class D addresses.
  – Each class D address identifies a group of hosts.
  – 28 bits define over 250 million groups.

• Best-effort delivery.
Group Membership

• Hosts (single or multiple processes) may join and leave group.
• Special, multicast routers perform multicast routing and packet forwarding.
  – Hosts belonging to multicast groups periodically send messages to the closest multicast router.
  – Multicast routers and hosts use IGMP (Internet Group Management Protocol) to exchange membership information.
IP Multicast Routing

• Use spanning trees.
• Modified distance vector protocol using unicast routing information.
  – Build one spanning tree per source, per group.
  – Or, one shared spanning tree per group.
  – Use pruning to remove parts of the tree that don’t have any multicast group members.
  – Use tunneling to cross regions that are not multicast capable.
The Main IPv6 Header

### Header Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>4</td>
</tr>
<tr>
<td>Traffic class</td>
<td>8</td>
</tr>
<tr>
<td>Flow label</td>
<td>8</td>
</tr>
<tr>
<td>Payload length</td>
<td>16</td>
</tr>
<tr>
<td>Next header</td>
<td>8</td>
</tr>
<tr>
<td>Hop limit</td>
<td>8</td>
</tr>
<tr>
<td>Source address</td>
<td>16</td>
</tr>
<tr>
<td>Destination address</td>
<td>16</td>
</tr>
</tbody>
</table>

- **Source address**: 16 bytes
- **Destination address**: 16 bytes
## IPv6 Extension Headers

<table>
<thead>
<tr>
<th>Extension header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop-by-hop options</td>
<td>Miscellaneous information for routers</td>
</tr>
<tr>
<td>Destination options</td>
<td>Additional information for the destination</td>
</tr>
<tr>
<td>Routing</td>
<td>Loose list of routers to visit</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>Management of datagram fragments</td>
</tr>
<tr>
<td>Authentication</td>
<td>Verification of the sender’s identity</td>
</tr>
<tr>
<td>Encrypted security payload</td>
<td>Information about the encrypted contents</td>
</tr>
</tbody>
</table>
Extension Headers (2)

- The hop-by-hop extension header for large datagrams (jumbograms).

<table>
<thead>
<tr>
<th>Next header</th>
<th>0</th>
<th>194</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jumbo payload length</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Extension Headers (3)

- The extension header for routing.

<table>
<thead>
<tr>
<th>Next header</th>
<th>Header extension length</th>
<th>Routing type</th>
<th>Segments left</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type-specific data
The Transport Layer

Tannenbaum Chapter 6
Level 5    -- **Application** Layer  
(rlogin, ftp, SMTP, POP3, IMAP, HTTP..)

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

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

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

Level 1    -- **Physical** Layer
The Transport Layer

- End-to-end.
  - Communication from source to destination host.
  - Only hosts run transport-level protocols.
  - Under user’s control as opposed to network layer which is controlled/owned by carrier.
The Transport Service

- Service provided to application layer.
- Transport entity: process that implements the transport protocol running on a host.
  - At OS kernel, user-level process, or network card.
The Transport Layer

TPDU = Transport Protocol Data Unit
Types of Transport Services

• Connection-less versus connection-oriented.
  – Connection-less service: no logical connections, no flow or error control.
  – Connection-oriented:
    • Based on logical connections: connection setup, data transfer, connection teardown.
    • Flow and error control.
Transport versus Network Layer

• Transport layer is “controlled” by user.
  – Ability to enhance network layer quality of service.
  – Example: transport service can be more reliable than underlying network service.
  – Transport layer makes standard set of primitives available to users which are independent from the network service primitives, which may vary considerably.