Section Overview

❖ Physical Layer
❖ Link Layer
❖ IP Layer
Physical Layer

Modulation Methods:
- Amplitude, Frequency, Phase

Latency:
- Transmission Delay
  - $\Delta t$ between the 1st bit on the wire and the last bit on the wire
- Propagation Delay
  - Time for bits to travel from one end to the other
- Bandwidth-Delay Product
Shannon Capacity

The maximum rate of information that can be transmitted over a channel of a specified bandwidth in the presence of noise without loss:

\[ C = B \times \log_2(1 + S/N) \]

C: Transmission rate  B: Bandwidth
S: Signal              N: Noise

⇒ Increasing Bandwidth is MUCH more effective than increasing Signal or decreasing Noise.
**Link Layer**

**Framing:**
- Byte Counting
- Byte Stuffing
- Bit Stuffing

**Error Detection/Correction:**
- **Hamming Distance**
  - The minimum number of bits to change from valid codeword to another

- **Parity Bit**
  - XOR corresponding bits

- **Retransmissions:**
  - Automatic Repeat reQuest (ARQ)
  - Stop-and-Wait & Sliding window
Multiple Access Problem

- **ALOHA**: Node just sends when it has traffic; if collision happens, wait for a random amount of time and try again. ⇔ Huge amount of loss under high load

- **CSMA (Carrier Sense Multiple Access)**: Listen before send. ⇔ Collision is still possible because of delay

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**: CSMA + Aborting JAM for the rest of the frame time ⇔ Minimum frame length of 2D seconds

- **CSMA “Persistence”**: CSMA + P(send) = 1 / N ⇔ Reduce the chance of collision

- **Binary Exponential Backoff (BEB)**: Doubles interval for each successive collision ⇔ Very efficient in practice
Hidden vs. Exposed Terminal Problem

- **Hidden Node Problem**: Node A and node C both want to send to node B. Since A and C are out of each other's range, they can't "see" each other. Collision could happen if A and C are transmit to B simultaneously.

- **Exposed Terminal Problem**: Node B wants to send to node A, node C wants to send to node D. B and C are near each other while A and D are far apart. B and C are afraid of interfering each other's transmission and would both "shut up."

- **Solution?** RTS-CTS Mechanism!
Switching

- **Backward Learning**: Learn the sender’s port by looking at the packets

- **Spanning Tree Solution**:
  - Elect the root node of the tree (Usually the switch with the lowest address)
  - Grow tree based on the shortest distance from the root
  - Ports not on the spanning tree are turned off
IP Layer

Datagram Model:
- Connectionless service
- Packets contain destination address
- Packets may use different paths
- Each router has a forwarding table keyed by ip address.

Virtual Circuit Model:
- Connection-oriented service
- Packets contain labels to identify the circuit
- Packets use the same path
- Each router has a forwarding table keyed by circuit
Breakdown of IP

- Bootstrapping (DHCP)
- Finding Link nodes (ARP)
- Really big packets (Fragmentation)
- Errors in the network (ICMP)
- Running out of addresses (IPv6, NAT)
DHCP

- **Purpose:** Automatically configure addresses

- **Steps of DHCP:**
  - The node broadcasts a DISCOVER message on the local network (255.255.255.255)
  - DHCP server responds with an OFFER message
  - The node sends a REQUEST message to the server, asking for an ip address
  - The server responds with an ACK message, assigning an ip address
NAT (Network Address Translation)

- **Purpose**: Provide a solution to the exhaustion of ipv4 addresses

<table>
<thead>
<tr>
<th>Private Address:</th>
<th>Router Address:</th>
<th>Server Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>12.11.8.1</td>
<td>18.21.9.22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAT Forwarding Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Address</td>
</tr>
<tr>
<td>192.168.1.2:12345</td>
</tr>
</tbody>
</table>
GOOD luck :)