Physical LAN segment

- Hosts connected on the same physical LAN segment
- Some subnet; L2 forwarding
- ARP (IP→MAC) L2 frame (S, D), send
- Scale?

Extending or Interconnecting LANS

- Why not just one big LAN?
  - Limited amount of supportable traffic: on single LAN, all stations must share bandwidth
  - Single collision domain
- Physical layer extension
  - Repeaters
    - copies (amplifies, regenerates) bits between LAN segments
- Link Layer extensions
  - Bridges - connects (2) LAN segments
  - Each segment is its own collision domain
  - receives, stores, forward (when appropriate) packets between LANs
  - Learn which host is connected on which interface
  - Forget about the mapping after certain TTL – soft state

Forwarding Algorithm

1. bridge receives every packet transmitted on every attached LAN
2. bridge stores for each packet
   - physical address of sender
   - port (incoming LAN segment) on which pkt was received
3. for each packet received on any port: lookup dest. physical address in table
   - if not found, flood onto all attached LANs
   - if found, forward only out to specified LAN
4. forwarding table deleted if not refreshed

Virtual LAN

- Extend subnets beyond physical LAN segments
- Separate broadcast domains by VLAN ID
- Hosts in the same subnet belong to the same VLAN ID
- Hosts in the same subnet can be in different physical LAN segments
- Broadcasts restricted to same VLAN only
- Ports on switch mapped to VLAN ID
Configuring the switch

- Ports configured at switch
- Hosts on same VLAN → same subnet
- IP addresses for hosts need to confirm to the subnet

VLAN logical grouping

- VLANs provide segmentation based on broadcast domains.
- VLANs logically segment switched networks based on the functions, departments, or applications regardless of the physical location or connections to the network.
- VLANs can be connected by switches
- Forwarding based on tagging (IEEE 802.1Q)

VLAN Types

- Port-based
  - Ports assigned to VLANS
- MAC-based
  - Each MAC address manually programmed
- IP-based
  - Port mapped to IP address/mask

VLAN Tagging

- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN.
- IEEE 802.1Q
**VLAN frame format**

- **ProtoID:** 0x8100 (16 bits)
- **VLANID:** 12 bits (4K different VLAN ids)

**VLAN Tagging**

- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN.
  - Additional TAG field added to ethernet frame
  - At the receiving switch, the Header is stripped and forwarded to the appropriate ports

**Inter VLAN routing**

- Sending frame from VLAN 1 to VLAN2
  - Layer 3 routing
  - VLAN1 sends frame to the default MAC address of router connected to VLAN1
  - Router does a lookup and forwards it along the interface connected to VLAN2

**Benefits of VLANs**

- Logical grouping
- Dynamically add or remove hosts
- Separate broadcast domains
- Security
**Multiple access channel partitioning**

- Static and predetermined allocation of channel access: independent of user activity
- Idle users may be assigned to the channel, in which case channel capacity is wasted
- Examples: TDMA, FDMA, CDMA

**Multiple Access Techniques TDMA/FDMA/CDMA**

- Allow multiple users to share a common transmission medium
- Techniques:
  - **TDMA**: Time division Multiple Access
    - The spectrum usage is divided in the time domain
    - People take turns using the spectrum (amount of time allocated is the slot time)
  - **FDMA**: Frequency division multiple access
    - The spectrum usage is divided in the frequency domain
    - People are assigned portions of the spectrum for their own use (portion of the spectrum is the channel)
  - **CDMA**: Code Division Multiple Access
    - The entire spectrum is used by everyone but in a coded format
    - The signal is spread and only the receiver who knows the code can recover the signal
    - Analogy: people talking in different languages all at the same time

**Spread Spectrum Techniques (Types of CDMA)**

- Two types of techniques exist
- **Direct sequence CDMA (DS-CDMA or DSSS)**
  - Each bit of the signal is replaced by a code (longer bit sequence)
    - A narrow band signal (R bps) is multiplied by a wideband signal (W bps)
    - Receiver who knows the code will recover the signal; for the rest it appears as random noise
    - Used in IEEE 802.11 Wavelan

**Example**

<table>
<thead>
<tr>
<th>Data</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>1010 1010</td>
</tr>
<tr>
<td>Output</td>
<td>0101 1010</td>
</tr>
</tbody>
</table>

Receiver uses the code and the received signal to recover original data
**Frequency hopping**

- Frequency sequence CDMA (FS-CDMA or FSSS)
- A single user's signal is spread out over a number of channels
  - (1011) is transmitted as f1, f9, f11, f13
  - The receiver who tunes to f1, f9, f11 and f13 in sequence will be able to recover the bit stream
  - Used in Blue tooth wireless technology

---

**802.11 Wireless Networking**

(Chapter 6.1-6.3)

- Basically wireless Ethernet
- Connects a number of computers in a wireless LAN
- Ad-hoc mode (AHM) as well as Access Point mode (APM) supported
- AHM - Only direct communication, no routing functionality
- APM - Computers connected to the Internet via an AP
- Typical mode of operation
- Access point name refers to a channel; a host connected to an AP tunes to the same channel as the AP

---

**802.11 Physical Layer**

- Operates in the ISM band
  - LBand 915 to 928 MHz and the SBand 2.4 to 2.4835 GHz band are used for 802.11
- Uses Direct Sequence Spread Spectrum (DSSS)
- Signal is sent in a "coded" form
  - Topic of a course in communications
- Initial versions were 1 to 2 Mbps. Now 802.11b is 11 Mbps
- 802.11g provides up to 54 Mbps (Phase and Amplitude Keying)
- 802.11n more range 100s of Mbps

---

**802.11 DSSS**

- 83 MHz divided into eleven 22 MHz wide stationary channels
  - At any point only 3 non-overlapping channels available
- Spreading sequence is 11 bit barker word
  - 1 is mapped to 1, -1, 1, 1, 1, -1, -1, 1, -1, -1
  - 0 is mapped to -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1
  - Same sequence is used by all hosts
  - Multiple access problem needs to be solved
- Input signal is spread to 22 MHz wide spectrum
- Duration of 1 chip is 1/11 microsecond or 1 Mchips/sec
- Different modulation schemes used to obtain different rates
  - Binary Phase Shift Keying (gives 1 Mbps), Quadrature PSK (gives 2 Mbps), QPSK with Complementary Code Keying (4 bits/symbol at chip rate of 1.375 Mbps), (instead of 11/ use 8 bit barker code) gives 4*1.375 = 5.5 Mbps and 8 bits/symbol gives 11 Mbps
**802.11 Access Control**

- Carrier sensing
  - Is the medium idle? → Wait for an amount of time (IFS), if still idle transmit
  - IFS = inter frame spacing
  - Is the medium busy? → Wait until current txm ends, wait (IFS), if idle wait for random amount of time, else wait until current txm ends and repeat
  - (exponential backoff for collisions)
  - If channel is found to be busy wait and start a backoff timer (min = 10 slots)

**Problems with Carrier Sensing**

- Hidden terminal problem
  - Z does not hear X, hence transmits to Y and collides with transmission from X
  - No carrier does not imply don't send

- Exposed terminal problem
  - W hears Y but can safely transmit to X
  - Carrier may not imply don't send

**Use of RTS, CTS**

- Sender sends a small packet RTS (request to send) before sending data
- Receiver sends CTS (clear to send)
- All potential senders hearing RTS waits until a CTS is heard from some receiver
- If no CTS, transmit
- If CTS, wait for a time for sender to send data
- Hear RTS, but no CTS, then send
  - Exposed terminal case
- Don't hear RTS, but CTS receiver is close, don't send
  - Hidden terminal case
802.11 frame: addressing

- **Address 1**: MAC address of wireless host or AP to receive this frame.
- **Address 2**: MAC address of wireless host or AP transmitting this frame.
- **Address 3**: MAC address of router interface to which AP is attached.
- **Address 4**: Used only in ad hoc mode.

802.11 Issues

- Very popular in buildings, public spaces
- Tremendous opportunities
- Free/unlicensed spectrum interference issues
- Security, privacy, authentication being added
- Nice features to have:
  - Roaming across networks
  - Remote authentication
  - Mobile access
Bluetooth

- A cable replacement technology
- Operates in the ISM band (2.4GHz to 2.8 Ghz)
- Range is 10 cm to 10 meters can be extended to 100 meters by use of power control
- Data rates up to 1 Mbps (721Kbps)
- Supposed to be low cost, single chip radio
- Ideal for connecting devices in close proximity (piconet)
  - Phone and earpiece
  - Computer and printer
  - Camera and printer/fax etc
- Can form personal area networks (piconet and scatternet)
- IEEE 802.15.1 standard

Personal area networks

- Piconet
  - Master/slave nodes
  - Master and up to 7 slaves
  - Master allocates channels
- Scatternet
  - Node may be master in one network and slave in another network
  - Allows devices to be shared in different networks

Bluetooth Radio Link

- IEEE 802.11 operates in the same band using DSSS
- Bluetooth uses Frequency Hopping
- 83.5 MHz channel is divided into 79 1-MHz channels
  - 1600 hops per second (stays at one frequency for 625 microsecs)
  - Hopping sequence is 16 or 32
  - Selected by the master based on its MAC address
  - Master can connect up to seven slaves to form a piconet
- All members of the piconet use the same hopping sequence

Bluetooth Packet Format

- Access code identifies control packet type
  - Channel access code, device access code, inquiry access code
- Header contains address (3 bits) and packet types (4 bits)
- Voice packets with different FEC rates
- Data packets with low bit rate and high bit rate (with varying FEC as well)
**Connection establishment**

- Inquiry
- Broadcast
- Connection
- Inquiry scan
- Response-FHS
- Inquiry response
- Page scan
- Unicast-DAC
- Slave response
- ACK-DAC
- FHS-sender
- ACK-DAC
- Connection

**Piconet**
- A set of Bluetooth devices connected to a master
- Scatternet: a set of piconets

**Bluetooth Link Formation**
- Master inquires who is around
- Active slaves respond and the master learns who is around
- Master pages slaves and informs them of hopping sequence, active member address
- Active slaves get packets when header matches active member address
- A link is formed between master and each slave
- Inactive slaves can go into "park" state and give up address

**Mobile IP**
- RFC 3344
- Has many features we've seen:
  - Home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- Three components to standard:
  - Indirect routing of datagrams
  - Agent discovery
  - Registration with home agent
Mobile IP: indirect routing

- Packet sent by home agent to foreign agent: a packet within a packet
- Permanent address: 128.119.40.186
- Care-of address: 79.129.13.2
- Packet sent by correspondent

Mobile IP: agent discovery

- Agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)

- H,F bits: home and/or foreign agent registration required
- 0 or more care-of-addresses

Mobile IP: registration example

- Home agent (HA): 128.119.40.186
- Foreign agent (COA): 79.129.13.2
- Visited network: 79.129.13/24
- Mobile agent (MA): 128.119.40.186
- Registration: required