Physical LAN segment

- Hosts connected on the same physical LAN segment
- Same 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 Types

- Port-based
  - Ports assigned to VLANS

- MAC-based
  - Each MAC address manually programmed

- IP-based
  - Port mapped to IP address/mask
- **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 Tagging

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

<table>
<thead>
<tr>
<th>bytes</th>
<th>Preamble 6</th>
<th>SFD 1</th>
<th>Destination Address 6</th>
<th>Source Address 6</th>
<th>Type/Length 2</th>
<th>Data Upto 1500</th>
<th>FCS 4</th>
</tr>
</thead>
</table>

**IEEE 802.3 Ethernet Frame Format**

<table>
<thead>
<tr>
<th>bytes</th>
<th>Preamble 6</th>
<th>SFD 1</th>
<th>Destination Address 6 bytes</th>
<th>Source Address 6 bytes</th>
<th>Tag 2 bytes</th>
<th>Type/Length 2 bytes</th>
<th>Data Upto 1500 bytes</th>
<th>FCS 4 bytes</th>
</tr>
</thead>
</table>

**IEEE 802.1Q Tag Insertion**

<table>
<thead>
<tr>
<th>bits</th>
<th>TPID 16</th>
<th>PCP 3</th>
<th>CFI 1</th>
<th>VID 12</th>
</tr>
</thead>
</table>

**IEEE 802.1Q Tag Format**

- **TPID** = Tag Protocol Identifier
- **PCP** = Priority Code Point
- **CFI** = Canonical Format Indicator
- **VID** = VLAN Identifies (VLAN ID)

- **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

Organize subnet hosts logically without being attached to the same physical segment

- 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
  - DS-CDMA and Frequency hopping CDMA
  - 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**

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 S Band 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 Mcps (instead of 11/ use 8 bit Barker code) gives 4*1.375 = 5.5 Mbps and 8bits/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 = 15 slots)
802.11 Access Control

- While the back off timer is running and channel becomes busy then stop timer and wait until channel becomes Idle
- ACKs and immediate response actions can be sent after SIFS (Short IFS) < IFS value used in multiple access control
- On a collision Double backoff timer value \( CWMIN++ \);
- Exponential backoff

Diagram:

- **Tx?**
  - **Idle?**
    - **Y**
      - **Have Data**
        - **Y**
          - **Wait IFS**
            - **Y**
              - **Idle?**
                - **N**
                  - **Wait EOT**
                - **S**
            - **S**
          - **N**
            - **Wait IFS**
              - **Y**
                - **Idle?**
                  - **N**
                    - **Wait IFS**
                  - **S**
                - **S**
            - **N**
              - **Idle?**
                - **N**
                  - **decr backoff**
                - **S**
        - **N**
          - **Wait EOT**
    - **F**
  - **Busy**

**Double Backoff timer**

**Idle Timer=0**
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 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

<table>
<thead>
<tr>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
<th>6</th>
<th>2</th>
<th>6</th>
<th>0 - 2312</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>frame control</td>
<td>duration</td>
<td>address 1</td>
<td>address 2</td>
<td>address 3</td>
<td>seq control</td>
<td>address 4</td>
<td>payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>

**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 frame: addressing

![Diagram showing the process of a 802.11 frame addressing in a network with an AP, H1, and R1.]
### 802.11 Frame: More

<table>
<thead>
<tr>
<th>Protocol Version</th>
<th>Type</th>
<th>Subtype</th>
<th>To AP</th>
<th>From AP</th>
<th>More frag</th>
<th>Retry</th>
<th>Power mgt</th>
<th>More data</th>
<th>WEP</th>
<th>Rsvd</th>
</tr>
</thead>
</table>

**Frame Type:** (RTS, CTS, ACK, data)

**Frame Seq #:** (for RDT)

**Duration of Reserved Transmission Time (RTS/CTS):**

**Frame Control:**

<table>
<thead>
<tr>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
<th>6</th>
<th>2</th>
<th>6</th>
<th>0 - 2312</th>
<th>4</th>
</tr>
</thead>
</table>

**Protocol Version:**

- 2
- 2
- 4
- 1
- 1
- 1
- 1
- 1
- 1
- 1
- 1
- 1

---

6-27
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

<table>
<thead>
<tr>
<th>72 bits</th>
<th>54 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Code</td>
<td>Header</td>
</tr>
<tr>
<td></td>
<td>Payload (2744 bits)</td>
</tr>
</tbody>
</table>

- **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 to Inquiry scan
- Inquiry scan to Inquiry response
- Page broadcast to Page scan
- Page scan to Page response
- Master response broadcast to Slave response
- Slave response to Connection
- 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:**
- dest: 128.119.40.186

**Foreign-agent-to-mobile packet**
- dest: 79.129.13.2
- dest: 128.119.40.186

**Foreign-agent-to-mobile packet**
- dest: 128.119.40.186

---

6-37
### Mobile IP: agent discovery

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

```
<table>
<thead>
<tr>
<th>type</th>
<th>code</th>
<th>checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

- H,F bits: home and/or foreign agent
- R bit: registration required

- 0 or more care-of-addresses

---

**Diagram:**
- Standard ICMP fields
- Mobility agent advertisement extension
- Type = 9
- Code = 0
- Checksum
- Router address
- Type = 16
- Length
- Sequence #
- Registration lifetime
- RBHFMGV
- Reserved
- 0 or more care-of-addresses
Mobile IP: registration example

visited network: 79.129.13/24

HA: 128.119.40.7
COA: 79.129.13.2
MA: 128.119.40.186
Lifetime: 9999
Identification: 714
encapsulation format

registration req.
COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
Identification: 714
encapsulation format

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format

registration req.
COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
Identification: 714

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714

Mobile agent
MA: 128.119.40.186

ICMP agent adv.
COA: 79.129.13.2
....