Wireless Networks
Wireless Networks Outline

- Terminology, WLAN types, IEEE Standards
  - IEEE 802.11a/b/g/n
- 802.11 AP Management Functions
  - Association, scanning
- 802.11 MAC Sub-Layer
  - DCF
    - CSMA/CA
    - MACAW
802.11 MAC Sub-Layer (cont.)
- RTS/CTS
- PCF
  • Beacons, DIFS, SIFS
- Frame Details
  • PLCP preamble and header
  • Address fields
- Dynamic Rate Adaptation
- Frame Fragmentation
802.3::

- Ethernet
- CSMA/CD

802.11a/b/g/n::

- **WiFi**
- CSMA/CA

802.15.4::

- **ZigBee** 802.11-based
  - lower data rates, lower power

**Bluetooth::**

- TDMA

- wireless **Personal Area Networks (PANs)** that provide secure, globally unlicensed short-range radio communication.
- Clusters with max of 8: cluster head + 7 nodes

**LAN, WLAN and WSN Terminology**
Elements of a Wireless Network

- **network infrastructure**
- **wireless hosts**
  - laptop, PDA, IP phone
  - run applications
  - may be stationary (non-mobile) or mobile
    - wireless does *not* always mean mobility
Elements of a Wireless Network

- **Network infrastructure**
  - Typically connected to a wired network.
  - Relay responsible for sending packets between wired network and wireless host(s) in its “area.”
    - E.g., cell towers, 802.11 access points.
Wireless Local Area Networks (WLANs)

- The proliferation of laptop computers and other mobile devices (PDAs and cell phones) created an *obvious* application level demand for wireless local area networking.

- Companies jumped in, quickly developing *incompatible* wireless products in the 1990's.

- Industry decided to entrust standardization to IEEE committee that dealt with wired LANs
  - *namely, the IEEE 802 committee!!*
IEEE 802 Standards Working Groups

<table>
<thead>
<tr>
<th>Number</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1</td>
<td>Overview and architecture of LANs</td>
</tr>
<tr>
<td>802.2</td>
<td>Logical link control</td>
</tr>
<tr>
<td>802.3 *</td>
<td>Ethernet</td>
</tr>
<tr>
<td>802.4</td>
<td>Token bus (was briefly used in manufacturing plants)</td>
</tr>
<tr>
<td>802.5</td>
<td>Token ring (IBM’s entry into the LAN world)</td>
</tr>
<tr>
<td>802.6</td>
<td>Dual queue dual bus (early metropolitan area network)</td>
</tr>
<tr>
<td>802.7</td>
<td>Technical advisory group on broadband technologies</td>
</tr>
<tr>
<td>802.8 †</td>
<td>Technical advisory group on fiber optic technologies</td>
</tr>
<tr>
<td>802.9</td>
<td>Isochronous LANs (for real-time applications)</td>
</tr>
<tr>
<td>802.10</td>
<td>Virtual LANs and security</td>
</tr>
<tr>
<td>802.11 *</td>
<td>Wireless LANs</td>
</tr>
<tr>
<td>802.12</td>
<td>Demand priority (Hewlett-Packard’s AnyLAN)</td>
</tr>
<tr>
<td>802.13</td>
<td>Unlucky number. Nobody wanted it</td>
</tr>
<tr>
<td>802.14</td>
<td>Cable modems (defunct: an industry consortium got there first)</td>
</tr>
<tr>
<td>802.15 *</td>
<td>Personal area networks (Bluetooth)</td>
</tr>
<tr>
<td>802.16 *</td>
<td>Broadband wireless</td>
</tr>
<tr>
<td>802.17</td>
<td>Resilient packet ring</td>
</tr>
</tbody>
</table>

Figure 1–38. The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up.
The following IEEE 802.11 standards exist or are in development to support the creation of technologies for wireless local area networking:

- **802.11a** - 54 Mbps standard, 5 GHz signaling (ratified 1999)
- **802.11b** - 11 Mbps standard, 2.4 GHz signaling (1999)
- **802.11c** - operation of bridge connections (moved to 802.1D)
- **802.11d** - worldwide compliance with regulations for use of wireless signal spectrum (2001)
- **802.11e** - Quality of Service (QoS) support (not yet ratified)
- **802.11f** - Inter-Access Point Protocol recommendation for communication between access points to support roaming clients (2003)
- **802.11g** - 54 Mbps standard, 2.4 GHz signaling (2003)
- **802.11h** - enhanced version of 802.11a to support European regulatory requirements (2003)
- **802.11i** - security improvements for the 802.11 family (2004)
- **802.11j** - enhancements to 5 GHz signaling to support Japan regulatory requirements (2004)
- **802.11k** - WLAN system management (in progress)
The following IEEE 802.11 standards exist or are in development to support the creation of technologies for wireless local area networking:

- **802.11m** - maintenance of 802.11 family documentation
- **802.11n** - OFDM version at 248 Mbps; MIMO version 600 Mbps **formally voted into the standard in September 2009**!
- **802.11p** - Wireless Access for the Vehicular Environment
- **802.11r** - fast roaming support via Basic Service Set transitions
- **802.11s** - ESS mesh networking for access points
- **802.11t** - Wireless Performance Prediction - recommendation for testing standards and metrics
- **802.11u** - internetworking with 3G / cellular and other forms of external networks
- **802.11v** - wireless network management / device configuration
- **802.11w** - Protected Management Frames security enhancement
- **802.11x** - skipped (generic name for the 802.11 family)
- **802.11y** - Contention Based Protocol for interference avoidance
Wireless Link Standards

Indoor
10-30m

Outdoor
50-200m

Mid-range outdoor
200m – 4 Km

Long-range outdoor
5Km – 20 Km

Data rate (Mbps)

.056
.384
5-11
4
1

802.15

802.11b

802.11a,g

802.11n

802.11a,g point-to-point

802.16 (WiMAX)

UMTS/WCDMA-HSPDA, CDMA2000-1xEVDO

UMTS/WCDMA, CDMA2000

IS-95, CDMA, GSM

3G cellular enhanced

2G

3G

Data

Advanced Computer Networks  Wireless Networks
Wireless Link Characteristics

Differences from wired link...

- **decreased signal strength**: radio signal attenuates as it propagates through matter (path loss).

- **interference from other sources**: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well.

- **multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different times.

.... makes communication across (even a point to point) wireless link much more difficult.
Classification of Wireless Networks

- **Base Station**: all communication through an *Access Point (AP)* {note hub topology}. Other nodes can be fixed or mobile.

- **Infrastructure Wireless**: AP is connected to the *wired* Internet.

- **Ad Hoc Wireless**: wireless nodes communicate directly with one another.

- **MANETs (Mobile Ad Hoc Networks)**: ad hoc nodes are mobile.
Figure 1-36. (a) Wireless networking with a base station. (b) Ad hoc networking.
(a) Infrastructure Wireless LAN
## Wireless Network Taxonomy

<table>
<thead>
<tr>
<th>Infrastructure (e.g., APs)</th>
<th>Single Hop</th>
<th>Multiple Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>No infrastructure</td>
<td>host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet</td>
<td>host may have to relay through several wireless nodes to connect to larger Internet: <em>mesh net</em></td>
</tr>
<tr>
<td></td>
<td>no base station, no connection to larger Internet (Bluetooth, ad hoc nets)</td>
<td>no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET</td>
</tr>
</tbody>
</table>
The 802.11 Protocol Stack

Figure 4-25. Part of the 802.11 protocol stack.

Note - ordinary 802.11 products are no longer being manufactured.

Tanenbaum
Wireless Physical Layer

- Physical layer conforms to OSI (five options)
  - 1997: **802.11** infrared, FHSS, DSSS {FHSS and DSSS run in the 2.4GHz band}
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
  - 2009: **802.11n** OFDM and MIMO

- **802.11 Infrared**
  - Two capacities: 1 Mbps or 2 Mbps.
  - Range is 10 to 20 meters and cannot penetrate walls.
  - Does not work outdoors.

- **802.11 FHSS (Frequency Hopping Spread Spectrum)**
  - The main issue is **multipath fading**.
  - [P&D] The idea behind spread spectrum is to spread the signal over a wider frequency to minimize the interference from other devices.
  - 79 non-overlapping channels, each 1 Mhz wide at low end of 2.4 GHz ISM band.
  - The same pseudo-random number generator used by all stations to start the hopping process.
  - Dwell time: min. time on channel before hopping (400msec).
Media Access Control

Logical Link Control

Contention-free service

Contention service

Point Coordination Function (PCF)

Distributed Coordination Function (DCF)

- 2.4-Ghz frequency-hopping spread spectrum (1 Mbps, 2 Mbps)
- 2.4-Ghz direct-sequence spread spectrum (1 Mbps, 2 Mbps)
- Infrared (1 Mbps, 2 Mbps)
- 5-Ghz orthogonal FDM (6, 9, 12, 18, 24, 36, 48, 54 Mbps)
- 2.4-Ghz direct-sequence spread spectrum (5.5 Mbps, 11 Mbps)
- 2.4-Ghz DS-SS (6, 9, 12, 18, 24, 36, 48, 54 Mbps)

IEEE 802.11  IEEE 802.11a  IEEE 802.11b  IEEE 802.11g
802.11 DSSS (Direct Sequence Spread Spectrum)

- The main idea is to represent each bit in the frame by multiple bits in the transmitted signal (i.e., it sends the XOR of that bit and $n$ random bits).
- Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Kurose & Ross Chap 6).
- Each bit transmitted using an 11-bit chipping Barker sequence, PSK at 1Mbaud.
- This yields a capacity of 1 or 2 Mbps.

**Figure 2.37 Example 4-bit chipping sequence**
Code Division Multiple Access (CDMA)

- Used in several wireless broadcast channels (cellular, satellite, etc) standards.
- A unique “code” assigned to each user; i.e., code set partitioning.
- All users share the same frequency, but each user has its own chipping sequence (i.e., code) to encode data.

- **encoded signal** = (original data) X (chipping sequence)

- **decoding**: inner-product of encoded signal and chipping sequence

- Allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”).
CDMA Encode/Decode

sender

data bits

code

slot 1

slot 0

d_1 = -1
d_0 = 1

channel output Z_{i,m} = d_i \cdot c_m

receiver

data code

received input

code

slot 1

slot 0

D_i = \sum_{m=1}^{M} Z_{i,m} \cdot c_m

M

d_1 = -1
d_0 = 1

slot 1 channel output

slot 0 channel output

Bit width
CDMA: Two-Sender Interference

senders

data bits

\[ d_0^1 = 1 \]

\[ d_0^2 = 1 \]

code

\[ \begin{array}{cccccc}
1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & -1 & -1 \\
\end{array} \]

\[ \begin{array}{cccccc}
1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & -1 & -1 \\
\end{array} \]

Z_{i,m}^1 = d_i^1 \cdot c_m^1

channel, Z_{i,m}^*

\[ \begin{array}{cccc}
2 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 \\
\end{array} \]

Z_{i,m}^2 = d_i^2 \cdot c_m^2

receiver 1

\[ d_i^1 = \sum_{m=1}^{M} Z_{i,m}^* \cdot c_m^1 \]

\[ d_0^1 = -1 \]

\[ d_0^2 = 1 \]

WPI
Advanced Computer Networks
Wireless Networks
Wireless Physical Layer

- **802.11a OFDM (Orthogonal Frequency Divisional Multiplexing)**
  - Compatible with European HiperLan2.
  - **54 Mbps** in wider 5.5 GHz band ➔ transmission range is limited.
  - Uses 52 FDM channels (48 for data; 4 for synchronization).
  - Encoding is complex (PSM up to 18 Mbps and QAM above this capacity).
  - E.g., at 54 Mbps 216 data bits encoded into 288-bit symbols.
  - More difficulty penetrating walls.
802.11b HR-DSSS (High Rate Direct Sequence Spread Spectrum)

- 11a and 11b shows a split in the standards committee.
- 11b approved and hit the market before 11a.
- Up to 11 Mbps in 2.4 GHz band using 11 million chips/sec.
- Note in this bandwidth all these protocols have to deal with interference from microwave ovens, cordless phones and garage door openers.
- Range is 7 times greater than 11a.
- 11b and 11a are incompatible!!
• 802.11g OFDM (Orthogonal Frequency Division Multiplexing)
  - An attempt to combine the best of both 802.11a and 802.11b.
  - Supports bandwidths up to 54 Mbps.
  - Uses 2.4 GHz frequency for greater range.
  - Is backward compatible with 802.11b.
## Data Rate vs Distance (m)

<table>
<thead>
<tr>
<th>Data Rate (Mbps)</th>
<th>802.11b</th>
<th>802.11a</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>90+</td>
<td>—</td>
<td>90+</td>
</tr>
<tr>
<td>2</td>
<td>75</td>
<td>—</td>
<td>75</td>
</tr>
<tr>
<td>5.5(b)/6(a/g)</td>
<td>60</td>
<td>60+</td>
<td>65</td>
</tr>
<tr>
<td>9</td>
<td>—</td>
<td>50</td>
<td>55</td>
</tr>
<tr>
<td>11(b)/12(a/g)</td>
<td>50</td>
<td>45</td>
<td>50</td>
</tr>
<tr>
<td>18</td>
<td>—</td>
<td>40</td>
<td>50</td>
</tr>
<tr>
<td>24</td>
<td>—</td>
<td>30</td>
<td>45</td>
</tr>
<tr>
<td>36</td>
<td>—</td>
<td>25</td>
<td>35</td>
</tr>
<tr>
<td>48</td>
<td>—</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>54</td>
<td>—</td>
<td>10</td>
<td>20</td>
</tr>
</tbody>
</table>
Wireless Physical Layer

- **802.11n OFDM version at 248 Mbps**

- **Physical Layer Changes:**
  - Multiple-Input-Multiple-Output (MIMO)
  - Maximum of 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.
  - Spatial Division Multiplexing (SDM)

- **MAC Layer Changes:**
  - Frame aggregation into single block for transmission
IEEE 802.11 MAC Frame Format

FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control
802.11 LAN Architecture

- Wireless host communicates with base station
  - Base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - Wireless hosts
  - Access point (AP): base station
  - Ad hoc mode: hosts only

BSS 1

BSS 2

Internet

Hub, switch or router

AP
802.11 Management Functions

- Channel Selection
- Scanning
- Station (user) Authentication and Association
- Beacon Management
- Power Management Mode
Channels and AP Association

- **802.11b**: 2.4GHz-2.485GHz spectrum divided into **11 channels** (overlapping frequencies).
  - AP admin chooses frequency for AP.
  - Interference is possible: The channel can be same as that chosen by a neighbor AP!
- **Wireless nodes must associate with an AP.**
  - Node scans channels, listening for beacon frames containing AP’s name (SSID) and MAC address.
  - Node makes choice for AP association {default is best RSSI}.
  - may perform authentication [K&R Chapter 8].
  - will typically run DHCP to get IP address in AP’s subnet.
802.11 Overlapping Channels

- 802.11b/g transmission occurs on one of 11 overlapping channels in the 2.4GHz North American ISM band.
802.11: Passive/Active Scanning

**Passive Scanning**
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: H1 to selected AP

**Active Scanning**
1. Probe Request frame broadcast from H1
2. Probes response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: H1 to selected AP
In 802.11 wireless LANs, “seizing the channel” does not exist as in 802.3 wired Ethernet.

Two additional problems:
- Hidden Terminal Problem
- Exposed Station Problem

To deal with these two problems, 802.11 supports two modes of operation:
- DCF (Distributed Coordination Function)
- PCF (Point Coordination Function).

All implementations must support DCF, but PCF is optional.
Figure 4-26. (a) The hidden terminal problem. (b) The exposed station problem.
The Hidden Terminal Problem

- Wireless stations have transmission ranges and not all stations are within radio range of each other.
- Simple CSMA will not work!
- C transmits to B.
- If A "senses" the channel, it will not hear C's transmission and falsely conclude that A can begin a transmission to B.
The Exposed Station Problem

- This is the inverse problem.
- B wants to send to C and listens to the channel.
- When B hears A’s transmission, B falsely assumes that it cannot send to C.
CSMA/CA (CSMA with Collision Avoidance) uses one of two modes of operation:

- virtual carrier sensing
- physical carrier sensing

The two methods are supported by:

1. **MACAW** (Multiple Access with Collision Avoidance for Wireless) with virtual carrier sensing.
2. 1-persistent physical carrier sensing.
MACA protocol reduces hidden and exposed terminal problems:

- Sender broadcasts a Request-to-Send (RTS) and the intended receiver sends a Clear-to-Send (CTS).
- Upon receipt of a CTS, the sender begins transmission of the frame.
- RTS, CTS helps determine who else is in range or busy (Collision Avoidance).
  - Can a collision still occur?
Wireless LAN Protocols

- **MACAW** added ACKs, Carrier Sense, and BEB done per stream and **not** per station.

Figure 4-12. (a) A sending an RTS to B. (b) B responding with a CTS to A.
Virtual Channel Sensing in CSMA/CA

Figure 4-27. The use of virtual channel sensing using CSMA/CA.

- **C** (in range of A) receives the RTS and based on information in RTS creates a virtual channel busy NAV (Network Allocation Vector).
- **D** (in range of B) receives the CTS and creates a shorter NAV.
Collision Avoidance: RTS-CTS Exchange

- RTS(A)
- RTS(B)
- reservation collision
- NAV defer
- DATA (A)
- ACK(A)
What is the advantage of RTS/CTS?

RTS is 20 bytes, and CTS is 14 bytes.

MPDU can be 2300 bytes.

- “virtual” implies source station sets the duration field in data frame or in RTS and CTS frames.

- Stations then adjust their NAV accordingly!
1-Persistent Physical Carrier Sensing

- The station *senses* the channel when it wants to send.
- If idle, the station transmits.
  - *A station does not sense the channel while transmitting.*
- If the channel is busy, the station defers until idle and then transmits (*1-persistent*).
- Upon collision (no ACK received), wait a *random time* using binary exponential backoff (*BEB*).
**IEEE 802.11 MAC Protocol: CSMA/CA**

### 802.11 sender

1. if sense channel idle for DIFS then
   - Transmit entire frame (no CD).
2. if sense channel busy then
   - Choose a random backoff time.
   - When channel is busy, counter is frozen.
   - Timer counts down while channel idle and transmit when timer expires.
   - if no ACK, increase random backoff interval, repeat 2.

### 802.11 receiver

- if frame received OK
  - return ACK after SIFS.
Point Coordinated Function (PCF)

- PCF uses a base station to **poll** other stations to see if they have frames to send.
- No collisions occur.
- Base station sends **beacon frame** periodically.
- Base station can tell another station to **sleep** to save on batteries and base stations holds frames for sleeping station.
- Subsequently, BS awakens sleeping node via **beacon frame**.
DCF and PCF Co-Existence

Distributed and centralized control can co-exist using InterFrame Spacing.

- **SIFS (Short IFS)**: the time waited between packets in an ongoing dialog (RTS, CTS, data, ACK, next frame)
- **PIFS (PCF IFS)**: when no SIFS response, base station can issue beacon or poll.
- **DIFS (DCF IFS)**: when no PIFS, any station can attempt to acquire the channel.
- **EIFS (Extended IFS)**: lowest priority interval used to report bad or unknown frame.
Inter-frame Spacing in 802.11

Figure 4-29. Interframe Spacing in 802.11.
Fig. 1  CSMA/CA protocol of IEEE 802.11 MAC DCF. [N. Kim]
802.11 Physical Layer

‘Adjust transmission rate on the fly’

Fig. 2 IEEE 802.11b HR/DSSS PHY framing structure.

[N. Kim]
### 802.11 Frames - Addresses

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

802.11 frame

802.3 frame

AP MAC addr | H1 MAC addr | R1 MAC addr

address 1 | address 2 | address 3

dest. address | source address

Advanced Computer Networks
Wireless Networks
802.11 Frame Addresses (more)

duration of reserved transmission time (RTS/CTS)

frame seq # (for RDT)

frame type
(RTS, CTS, ACK, data)
802.11: Mobility within Same Subnet

- **H1** remains in same IP subnet: IP address can remain same.
- **Switch**: Which AP is associated with H1?
  - Uses self-learning (Ch. 5)
  - Switch will see frame from H1 and “remember” which switch port can be used to reach H1.
Wireless Network Details

- All APs (or base stations) will periodically send a beacon frame (10 to 100 times a second).

- Beacon frames are also used by DCF to synchronize and handle nodes that want to sleep.
  - Node sets Power management bit to indicate going to sleep and timer wakes node up for next beacon.
  - The AP will buffer frames intended for a sleeping wireless client and wakeup for reception with beacon frame.

- AP downstream/upstream traffic performance is asymmetric.

- Wireless communication quality between two nodes can be asymmetric due to multipath fading. (Characterization paper shows this!)
802.11b, g and n use **dynamic rate adaptation** based on frame loss (algorithms internal to wireless card at the AP)

- e.g. for 802.11b choices are: 11, 5.5, 2 and 1 Mbps

- Standard 802.11 retries:
  - 7 retries for RTS and CTS
  - 4 retries for Data and ACK frames

- RTS/CTS may be turned off by default

  [Research has shown that RTS/CTS degrades performance when hidden terminal is not an issue].
Node Contention

Fig. 7  Throughputs with node contentions.

[58] [N. Kim]

Advanced Computer Networks  Wireless Networks
Wireless Link Characteristics

SNR: signal-to-noise ratio
- larger SNR – easier to extract signal from noise.

SNR versus BER tradeoffs
- given a physical layer: increase power -> increase SNR -> decrease BER.
- given a SNR: choose physical layer that meets BER requirement, aiming for highest throughput.

SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate).
**Dynamic Rate Adaptation**

**Mobile Node Example:**

1. SNR decreases, BER increases as node moves away from base station.

2. When BER becomes too high, switch to lower transmission rate but with lower BER.

**Idea:** lower data rate for higher throughput.

**Note** - Performance Anomaly paper shows there are other issues when wireless flows contend at AP!
Fig. 6. Throughput comparison of our proposed rate adaptation scheme (CARA-1) against RTS/CTS, ARF, and single-rate schemes for one-to-one topology networks with various distance ($r$)
- High wireless error rates $\Rightarrow$ long packets have less probability of being successfully transmitted.

- Solution: MAC layer fragmentation with stop-and-wait protocol on the fragments.

Figure 4-28 Fragmentation in 802.11
Wireless Networks Summary

- Terminology, WLAN types, IEEE Standards
  - Infrastructure, ad hoc, MANET, Base Station, Access Point, single and multi-hop

- IEEE 802.11a/b/g/n
  - Differences in data rate and transmission technologies
  - FHSS, DSSS, CDMA, OFDM, HR-DSSS, MIMO
Wireless Networks Summary

- **802.11 AP Management Functions**
  - Association with AP, active and passive scanning, beacon frames

- **802.11 MAC Sub-Layer**
  - Overlapping channels
  - Hidden terminal problem, exposed station problem
  - DCF
    - CSMA/CA
    - MACAW
Wireless Networks Summary

- 802.11 MAC Sub-Layer (cont.)
  - RTS/CTS
  - PCF
    - Beacons, DIFS, SIFS, sleeping nodes
  - Frame Details
    - PLCP preamble and header
    - 3 or 4 Address fields used in 802.11
  - SNR vs BER issues
  - Dynamic Rate Adaptation
  - Frame Fragmentation