Wireless Local Area Networks
Wireless Local Area Networks

• 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.
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.
Wireless LANs

Figure 1-36. (a) Wireless networking with a base station. (b) Ad hoc networking.
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.
Wireless Physical Layer

• Physical layer conforms to OSI (five options)
  – 1997: 802.11 infrared, FHSS, DHSS
  – 1999: 802.11a OFDM and 802.11b HR-DSSS
  – 2001: 802.11g OFDM

• 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 (Frequence Hopping Spread Spectrum)
  – The main issue is multipath fading.
  – 79 non-overlapping channels, each 1 Mhz wide at low end of 2.4 GHz ISM band.
  – Same pseudo-random number generator used by all stations.
  – Dwell time: min. time on channel before hopping (400msec).
Wireless Physical Layer

• **802.11 DSSS (Direct Sequence Spread Spectrum)**
  – Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Tanenbaum sec. 2.6.2).
  – Each bit transmitted using an 11 chips Barker sequence, PSK at 1Mbaud.
  – 1 or 2 Mbps.

• **802.11a OFDM (Orthogonal Frequency Divisional Multiplexing)**
  – Compatible with European HiperLan2.
  – 54Mbps 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 54Mbps 216 data bits encoded into into 288-bit symbols.
  – More difficulty penetrating walls.
Wireless Physical Layer

- **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!!
Wireless Physical Layer

• **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.
802.11 MAC Sublayer Protocol

• 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 “\textit{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.
Distribute Coordination Function (DCF)

- Uses **CSMA/CA** (*CSMA* with *Collision Avoidance*).
  - Uses one of two modes of operation:
    - *virtual carrier sensing*
    - physical carrier sensing

- The two methods are supported:
  1. **MACAW** (Multiple Access with Collision Avoidance for Wireless) with virtual carrier sensing.
  2. 1-persistent physical carrier sensing.
Wireless LAN Protocols

[Tan pp. 269-270]

- **MACA** protocol solved 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.
Virtual Channel Sensing in CSMA/CA

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 \textit{duration field} in data frame or in RTS and CTS frames.

• Stations then adjust their NAV accordingly!
• High wireless error rates ➞ long packets have less probability of being successfully transmitted.
• Solution: MAC layer fragmentation with stop-and-wait protocol on the fragments.
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, wait a *random time* using binary exponential backoff.
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.
DCF and PCF Co-Existence

• Distributed and centralized control can co-exist using InterFrame Spacing.
• SIFS (Short IFS) :: is 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.
Figure 4-29. Interframe Spacing in 802.11.
Wireless Card Implementation Details

• 802.11b and 802.11g use *dynamic capacity adaptation* based on ?? (internal to wireless card at the AP)
  – e.g. for 802.11b choices are: 11, 5.5, 2 and 1 Mbps
• RTS/CTS may be turned off by default.
• All APs (or base stations) will periodically send a beacon frame (10 to 100 times a second).
• AP downstream/upstream traffic performance is asymmetric.
• Wireless communication quality between two nodes can be asymmetric due to multipath fading.