Wireless LAN Standards

802.11 and variants
HiperLAN and HiperLAN/2

IEEE 802 Group
- Develops LAN/MAN standards
- Individual working groups focus on specific areas, e.g.,
  - 802.3 also called Ethernet
  - 802.11 the wireless LAN standard
  - 802.15 the wireless PAN standard

IEEE 802.11 Wireless LAN
- Formed in 1990
- Defines the PHY and MAC layer
- Frequency bands used are in ISM or U-NII bands
- Represents the first standard for WLANs
- Before: application specific proprietary products (may have better performance for the given application but vendor specific and expensive)
- Originally to develop standard for data rates of 1Mbps and 2Mbps - released in 1997.

IEEE 802.11 Evolution

<table>
<thead>
<tr>
<th>Standard</th>
<th>Approved</th>
<th>Frequency Bands</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>September 1999</td>
<td>5.15-5.25GHz, 5.25-5.35GHz, 5.725-5.825GHz</td>
</tr>
<tr>
<td>802.11b</td>
<td>February 1999</td>
<td>2.4GHz</td>
</tr>
<tr>
<td>802.11g</td>
<td>July 1999</td>
<td>2.4GHz, 5GHz</td>
</tr>
</tbody>
</table>

802.11g: not released yet, backwards compatible with 802.11b, defines symbol rates up to 54Mbps using OFDM

IEEE 802.11 Wireless LAN
- Two kinds of operation:
  - Ad hoc
    - IBSS (Independent Basic Service Set)
  - Client-server
    - Infrastructure mode (basic service set)
- A BSS (Basic Service Set) is a working group of at least two nodes (or stations – STA)

802.11 PHY
- Originally 3 different channel options:
  - Infra-red
  - Frequency Hopping Spread Spectrum (FHSS) 2.4GHz
  - Direct Sequence Spread Spectrum (DSS) 2.4GHz
- Radiated power is limited
  - 1W in the US (for radio) – limited more
  - ~20mW in Europe, 1mW in Japan (for radio)
802.11 Infrared PHY
- Not really used – IrDA is more common and cheap.
- Provides data rates of 1Mbps and 2Mbps
- Max output power is 2W
- Works in the ~900nm range (regular IR LED)

802.11 FHSS PHY
- 22 hop patterns to choose from
- 79 hopping frequencies
- 1 or 2 Mbps
- Some early products favored it because it is less prone to interference.
- Not really used anymore since it can not scale well with higher symbol rates.
- 20msec dwell time -> 50 hops/sec

802.11 DSS PHY
- 3 separate channels in the 80MHz wide band of the 2.4GHz ISM – each 20MHz wide.
- Baker sequence (PN-sequence) to modulate the data stream (to spread the spectrum).
- Not to be confused with CDMA! Here the PN sequence is fixed for all stations and published in the standard, thus DSS – originally used for encryption – is only used to spread energy.
- 1 or 2 Mbps symbol rate.

802.11 MAC layer
- Two access functions defined.
  - The default is: Distributed Coordination Function (DCF) and is CSMA/CA based.
  - The optional access method is the Point Coordination Function (PCF) . Only to be used in the infrastructure mode. Based on a TDMA polling scheme.

Distributed Coordination Function (DCF) - CSMA/CA
- All stations have to be equipped with DCF. The DCF can be used in both the IBSS and infrastructure modes.
- STAs have to monitor the channel. If the channel is busy, stations have to back-up for a random time.
- RTS – CTS message exchange for CA.
- ACK packets for fast arq after data transmission.

CSMA
- A station desiring to transmit has to sense the medium. If the medium is busy the station will defer its transmission for a later time. If the medium is free, the station can go ahead and transmit.
- Collision Avoidance is needed (Detection cannot be used)
**CSMA/CA**

- If the medium is free for a specific time duration (DIFS – Distributed Inter Frame Space) then the station can transmit.
  - This enables radio propagation delay
  - Also, since time is not slotted, nodes will not know the difference between a free channel or a temporary free (e.g., between an RTS and CTS or data and ACK) channel otherwise.

**Virtual Carrier Sense**

- A fancy name for RTS/CTS exchange or CA.
- A station contending for the channel sends out an RTS message first. RTS contains the destination and the required time needed for the entire transmission process.
- The CTS response will contain the duration of the transmission process too, thus all nodes that are susceptible for a hidden terminal interference can keep a timer for the duration of this transmission.

**The virtual carrier sense indicator is also called Network Allocation Vector.**

**Physical carrier sensing** and the virtual carrier sensing functions will provide the nodes the information about the channel’s state.

**Time between RTS-CTS-data-ACK** has to be smaller than DIFS, and is maximized in SIFS (Short Inter Frame Space)

**Back-off** is based on BEB (Binary Exponential Back-off).

If nodes are backed-off and the channel is empty for at least DIFS, then they start decrementing their back-off counter with a given frequency.

**DCF**

- "Collision Detection" is employed by the use of ACK packets after each transmission (and CRC check).
- Exceptions are the multicast transmissions.
- Thus the MAC layer provides with guaranteed delivery.
In a wireless environment it is more error-safe and efficient to transmit short packets:
- Higher BER of wireless
- Retransmission times should be considered
- Shorter messages can have better FEC.
Since Ethernet packets can be up to ~1500 bytes long it would be beneficiary if WLAN could provide the same size.

802.11 uses a simple F&R:
- Larger PDUs can be divided up into smaller fragments and sent one-by-one.
- Fragments have to arrive ordered – a station cannot send a new segment until the previous one has been acknowledged.
- If a fragment has been retransmitted too many times, the entire frame has to be dropped.

If a station wants to join an existing BSS, it needs to be synchronized to the AP. This can happen in two ways:
- Passive scanning: a station is scanning the channel for a beacon frame (a periodic frame sent by the AP for synchronization)
- Active scanning: the station tries to find an AP by transmitting Probe Request frames, waiting for a Probe Response.

Performance trade offs

Once a station has found an Access Point and decided to join the BSS, it will go through the optional authentication process
- Authentication is based on the knowledge of a password or encryption key

Once a station is authenticated, it will start the association process, which is the exchange of information about the BSS capabilities (e.g., roaming).
- Only after the association is completed can a station transmit and receive data frames.
Power Saving

- Battery power is a scarce resource in mobile equipment using WLANs.
- Stations in the infrastructure mode can go into a Power Saving Mode.
- The AP maintains a record of the stations in the power saving mode and buffers packets until the stations poll the AP for it or change their mode.

Power Saving

- APs periodically transmit beacon frames (for synchronization). This beacon frames also include information on which stations have back-logged packets waiting.
- Stations in the power saving mode monitor beacon transmissions, awake and "poll" the AP for these packets.
- Multicast messages are transmitted at an a priori known time, where all stations who wish to receive these information should wake up.

Short Inter Frame Space

- SIFS
  - To separate transmission belonging to the same dialogue.
  - Radio switch over times have to be calculated.
  - Set to 28µs in 802.11

Point Coordination IFS

- Used to give priority access to Point Coordinator (PC).
- Only the Point Coordinator can access a channel between SIFS and DIFS.
- Set to SIFS + a virtual slot time (the time the back-off counter is working), thus its value is 78µs in 802.11.

Distributed IFS

- For stations that wait for a free channel to contend.
- Set to PIFS + a virtual slot time, thus 128µs in 802.11.
**Extended IFS**

- A node that receives a non-decodable (e.g., due to collision of two RTS messages) message has to wait at least EIFS time before it can access the channel again.

**Frame Types**

- Data Frames
- Control Frames (e.g., RTS, CTS, ACK)
- Management Frames (exchanged the same way as data frames but are not reported to the higher layer).

**Frame Format for All Frames**

<table>
<thead>
<tr>
<th>Preamble</th>
<th>PLCP Header</th>
<th>MAC Data</th>
<th>CRC</th>
</tr>
</thead>
</table>

- PLCP Header (has to be transmitted with 1Mbps)
  - Length Word – number of bytes in this packet (good for PHY)
  - Signalling Field – for data speed
  - HEC – 16 bit CRC for the header

- General MAC Data and CRC

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration or ID</th>
<th>Addr. 1</th>
<th>Addr. 2</th>
<th>Addr. 3</th>
<th>Sequnc. Control</th>
<th>Addr. 4</th>
<th>Frame Body</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>
Frame Control Field

- Protocol Version:
  - To differentiate between, e.g., 802.11, 802.11a,b,e,g,h,i

- Type and Subtype
  - Define the type of the frame (management (e.g., beacon, probe, association), control (e.g., RTS, CTS, Poll, ACK), or Data). There are more than 30 different types of frames defined.

- ToDS
  - 1 In case the AP is not the final destination but the Distribution System

- FromDS
  - 1 In case the frame is coming from the DS

- More fragments
  - To signal more incoming fragments

- Retry
  - 1 If it is a retransmission fragment

- Power Management
  - To signal that station is changing from Active to power save mode (or vice-versa)

- More Data
  - There are more frames buffered to this station (for polling or changing status)

- WEP
  - Indicates that the frame body is encrypted with WEP

- Order
  - The frame is in a stream that is strictly ordered (for legacy applications – DEC’s LAT)
Frame Format for All Frames

<table>
<thead>
<tr>
<th>Preamble</th>
<th>PLCP Header</th>
<th>MAC Data</th>
<th>CRC</th>
</tr>
</thead>
</table>

- **General MAC Data and CRC**

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration or ID</th>
<th>Addr. 1</th>
<th>Addr. 2</th>
<th>Addr. 3</th>
<th>Sequnc. Control</th>
<th>Addr. 4</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>
</tr>
<tr>
<td>2312</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

MAC Data Fields

- **Duration/ID**
  - Duration used for NAV calculation
  - (or station ID for power save polling)
- **Sequence Control**
  - Frame numbering and fragment numbering
- **CRC**
  - 32 bits

Address Fields

- **Address-1**
  - Recipients Address (if TODS is not set this is the AP if it is set then the address of the end station)
- **Address-2**
  - Transmitters Address (if FromDS then address of AP, else the address of source)

- **Address-3**
  - If FromDS is set then the original source address, if ToDS is set, then the final destination
- **Address-4**
  - For the wireless distribution system, where a frame is transmitted from one Access point to another

Example: RTS Frame

- **RA**: Intended immediate recipient
- **TA**: The station transmitting this frame
- **Duration**: (in μs) the time required to transmit the next (data) frame plus a CTS frame plus an ACK frame and three SIFSs

Example: CTS Frame

- **RA**: The TA field of the RTS message
- **Duration**: (in μs) the duration value of the previous RTS frame minus a CTS time minus one SIFS.
Example: ACK Frame

<table>
<thead>
<tr>
<th>octets:</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Duration</td>
<td>RA</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>

MAC Header
- RA: is copied from the Address –2 field of the previous frame
- Duration: set to 0 if More Fragment bit was 0, otherwise the duration of the previous frame minus an ACK time minus one SIFS.

802.11 Task Groups

802.11b (Task Group b)
- Standard accepted in 1999.
- Most popular WLAN standard today.
- The WECA (Wireless Ethernet Compatibility Alliance or Wi-Fi Alliance) adopted 802.11b and renamed it Wi-Fi 2.4GHz (Wireless Fidelity).
- MAC is identical to that of 802.11
- PHY is solely 2.4GHz DSS, with rates: 11, 5.5, 2, 1Mbps.

802.11a (Task Group a)
- Standard accepted in 1999. People had to wait for products for more than 2 years.
- Quickly emerging.
- WECA adopted it as Wi-Fi 5.2GHz.
- MAC is identical to that of 802.11
- PHY is (Code) Orthogonal Frequency Division Multiplexing (OFDM) at 5.2GHz.
- Symbol rates of 54, 48, 36, 24, 12, 9, 6Mbps.
- 8 independent channels.

802.11a Physical (OFDM)
- Channels are of 20MHz
- Each channel has 52 "narrow-band" 300kHz carriers, (used by one station at a time)
- 108Mbps is enabled using two channels simultaneously.
Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

- Power consumption is similar, although it takes 4 to 9 times less energy to transmit a given length packet (due to speed) with 802.11a.
- 8 independent channels with 802.11a compared to 3 for Wi-Fi for cellular networks.
- Max data speed is 5 to 10 times higher.

Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

- Wi-Fi 5.2GHz has no other equipment interfering with it (yet), including microwave ovens. Can co-exist with Bluetooth or Wi-Fi 2.4GHz.
- Atheros claims, that during real measurements, the throughput of 802.11b never superseded that of 802.11a (in a typical office environment - despite the higher frequency band usage) – see diagrams on next pages.

Wi-Fi 2.4GHz vs. Wi-Fi 5.2GHz

**Cells and Co Channel Interference**

**802.11a vs. Wi-Fi**

**8 Cell System – Average Cell Throughput**
802.11a vs. Wi-Fi

MAC remains the same as 802.11
PHY to be backwards compatible with Wi-Fi 2.4GHz, thus at 2.4GHz.
High symbol rate modes of up to 54Mbps using OFDM, lower speeds up to 11Mbps using DSS. I took long to reach a common agreement.
Final specification expected soon.

802.11g

There were strong European concerns that 802.11a could interfere with NATO satellites and microwave radar systems.
To avoid such interference, two extensions to the PHY of 802.11a were added in 802.11h:
- the capability to select the employed channel automatically based upon observations (DFS – Dynamic Frequency Selection)
- ensuring the enforcement of strict radio power control (TPC – Transmit Power Control)

802.11h

IEEE802.11.e: wireless extension to IEEE802.1D enabling bridging using IEEE802.11
IEEE802.11.d deals with including country specific information into the beacon transmissions, so STAs are informed what part of the spectrum is available and what radio constraints they have to obey to (e.g., maximum transmission power).
IEEE802.11.f is defining a standard inter access point communication protocol for users roaming between access points (irrelevant to ad hoc networks).
IEEE802.11.i addresses the flaws of WEP, improving the wireless security at the MAC layer.

ETS I HiperLAN
**HiperLAN**

- European effort for WLAN standardization (superior to 802.11)
- HiperLAN is defined to work in the 5.2GHz U-NII.
- TDMA based access method.
- No commercial products.

**HiperLAN/2**

- New version of HiperLAN.
- Superior to any of the 802.11 versions.
- PHY is the same as that of 802.11h (similar to 802.11a).
- MAC layer is based on TDMA and is said to be Wireless-ATM-like.
- QoS provisioning.
- Infrastructure and ad hoc modes.
- Engineered to work with 3G and other systems.
- No products yet.