IEEE 802.11

- Wireless LAN standard specifying a wireless interface between a client and a base station (or access point), as well as between wireless clients
- Defines the PHY and MAC layer (LLC layer defined in 802.2)
  - Physical Media: radio or diffused infrared
- Standardization process begun in 1990 and is still going on (1st release '97, 2nd release '99, then '03, '05, ...)
IEEE 802.11 PHY Layer Activities

**PHY Layer**

- **IR**
- **2.4GHz FHSS**
- **2.4GHz DSSS**
- **5GHz OFDM**
- **802.11d / TG d Regulatory Domain Update**

- **802.11 1-2Mbps**
- **802.11 1-3Mbps**
- **802.11 1-2Mbps**
- **802.11b 5-11Mbps**
- **802.11a 6-54Mbps**
- **802.11g 2.4GHz OFDM 54Mbps** (approved in June'03)
- **802.11h 5GHz Spectrum Management**

IEEE 802.11 MAC Layer Activities

**MAC Layer**

- **802.11 MAC**
- **802.11e / TG e MAC Enhanced QoS**
- **802.11f / TG f Inter-AP Protocol**
- **802.11i / TG i Security Mechanisms**
- **802.11n/TG n High Throughput**
- **802.11p/TG p Mobility/Vehicular**
- **802.11s / TG s Mesh Networking**

802.11 Architecture

- **BSS (Basic Service Set):** set of nodes using the same coordination function to access the channel
- **BSA (Basic Service Area):** spatial area covered by a BSS (WLAN cell)
- **BSS configuration mode**
  - **ad hoc mode**
  - with infrastructure: the BSS is connected to a fixed infrastructure through a centralized controller, the so-called Access Point (AP)
WLAN with Infrastructure

- BSS contains:
  - wireless hosts
  - access point (AP): base station
- BSSs interconnected by distribution system (DS)

Ad Hoc WLANs

- Ad hoc network: IEEE 802.11 stations can dynamically form a network without AP and communicate directly with each other
- Applications:
  - "laptop" meeting in conference room, car
  - interconnection of "personal" devices
  - battlefield
- IETF MANET (Mobile Ad hoc Networks) working group

Extended Service Set (ESS)

- Several BSSs interconnected with each other at the MAC layer
- The backbone interconnecting the BSS APs (Distribution System) can be a:
  - LAN (802.3 Ethernet/802.4 token bus/802.5 token ring)
  - wired MAN
  - IEEE 802.11 WLAN, possibly meshed (routing problems!)
- An ESS can give access to the fixed Internet network through a gateway node
  - If fixed network is a IEEE 802.X, the gateway works as a bridge thus performing the frame format conversion
Possible Scenarios (1)

Ad hoc networking
Independent BSS (IBSS)

Network with infrastructure

Possible Scenarios (2)

Ad hoc WLAN

WLANs with infrastructure

Joining a BSS

- BSS with AP: Both authentication and association are necessary for joining a BSS
- Independent BSS: Neither authentication nor association procedures are required for joining an IBSS
Joining BSS with AP: Scanning

A station willing to join a BSS must get in contact with the AP. This can happen through:

1. **Passive scanning**
   - The station scans the channels for a Beacon frame (with sync. info) that is periodically sent by the AP

2. **Active scanning (the station tries to find an AP)**
   - The station sends a ProbeRequest frame
   - All AP's within reach reply with a ProbeResponse frame

Joining BSS with AP: Authentication

Once an AP is found/selected, a station goes through authentication

- **Open system authentication** (default, 2-step process)
  - Station sends authentication frame with its identity
  - AP sends frame as an ack / nack

- **Shared key authentication**
  - Stations receive shared secret key through secure channel independent of 802.11
  - Stations authenticate through secret key (requires encryption via WEP)

Joining BSS with AP: Association

Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming

- **STA → AP**: AssociateRequest frame
- **AP → STA**: AssociationResponse frame
- New AP informs old AP via DS
- Only after the association is completed, a station can transmit and receive data frames
Physical Layer

Three different access techniques:

- Infrared (IR)
- Frequency hopping spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)

Infrared

- Works in the regular IR LED range, i.e. 850-950 nm
- Used indoor only
- Employes diffusive transmissions, nodes can receive both scattered and line-of-sight signals
- 2 Mbps obtained through 4-pulse position modulation (4-PPM), i.e., 2 information bits encoded with 4 bits
- Max output power: 2W
- Not really used - IrDA is more common and cheaper
Spread Spectrum

• **Idea:** spread signal over wider frequency band than required
• **Frequency Hopping:** transmit over random sequence of frequencies
• **Direct Sequence**
  random sequence (known to both sender and receiver), called **chipping code**

FHSS

• Not really used anymore
• Frequency band: ISM @ 2.4 GHz
• In the U.S., the FCC has specified 79 ISM frequency channels with width equal to 1 MHz. Central frequency is @ 2.402 GHz
• 3 channels each corresponding to 1Mbps with GFSK modulation
• 20 ms dwell time $\Rightarrow$ 50 hop/s

DSSS (1)

• Radiated power is limited
  • Typical values: 85 mW
  • Maximum EIRP: 100mW EU, 1W USA
• Frequency band: ISM bands @ 2.4 GHz
• Band divided into 11 (USA) / 13(EU) overlapping channels
• 3 non overlapping channels, each 11MHz wide and with spacing 25MHz
IEEE 802.11 (Radio) Evolution

<table>
<thead>
<tr>
<th></th>
<th>802.11</th>
<th>802.11b (Wi-Fi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard approval</td>
<td>July 1997</td>
<td>Sep. 1999</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>83.5 MHz</td>
<td>83.5 MHz</td>
</tr>
<tr>
<td>Frequency of operation</td>
<td>2.4-2.4835 GHz</td>
<td>2.4-2.4835 GHz</td>
</tr>
<tr>
<td>Number of non-overlapping channels</td>
<td>3 Indoor/Outdoor</td>
<td>3 Indoor/Outdoor</td>
</tr>
<tr>
<td>Data rate per channel</td>
<td>1.2 Mbps</td>
<td>1.2, 5, 11 Mbps</td>
</tr>
<tr>
<td>Physical layer</td>
<td>FHSS, DSSS</td>
<td>DSSS</td>
</tr>
</tbody>
</table>

IEEE 802.11 MAC Protocol

Performs the following functions:
- Resource allocation
- Data segmentation and reassembly
- MAC Protocol Data Unit (MPDU) address
- MPDU (frame) format
- Error control

MAC Frames

Three frame types are defined
1. **Control**: positive ACK, handshaking for accessing the channel (RTS, CTS)
2. **Data Transfer**: information to be transmitted over the channel
3. **Management**: connection establishment/release, synchronization, authentication. Exchanged as data frames but are not reported to the higher layer
Data Transfer

- Asynchronous data transfer for delay-tolerant traffic (like file transfer)
  - DCF (Distributed Coordination Function)

- Synchronous data transfer for real-time traffic (like audio and video)
  - PCF (Point Coordination Function): based on the polling of the stations and controlled by the AP (PC)
  - Its implementation is optional (not really implemented)

Time Slot

- Time is divided into intervals, called slots
- A slot is the system unit time and its duration depends on the implementation of the physical layer
  - 802.11b: 20μs
- Stations are synchronized with the AP in the infrastructure mode and among each other in the ad hoc mode ⇒ the system is synchronous
- Synchronization maintained through Beacon frames

IFS

- Interframe space (IFS)
  - time interval between frame transmissions
  - used to establish priority in accessing the channel
- 4 types of IFS:
  - Short IFS (SIFS)
  - Point coordination IFS (PIFS) > SIFS
  - Distributed IFS (DIFS) > PIFS
  - Extended IFS (EIFS) > DIFS
- Duration depends on physical level implementation
**Short IFS (SIFS)**

- To separate transmissions belonging to the same dialogue
- Associated to the highest priority
- Its duration depends on:
  - Propagation time over the channel
  - Time to convey the information from the PHY to the MAC layer
  - Radio switch time from TX to RX mode
- $802.11b$: $10\mu s$

**Point Coordination IFS (PIFS)**

- Used to give priority access to Point Coordinator (PC)
- Only a PC can access the channel between SIFS and DIFS
- $\text{PIFS} = \text{SIFS} + 1$ time slot

**Distributed IFS (DIFS)**

- Used by stations waiting for a free channel to contend
- Set to: $\text{PIFS} + 1$ time slot
Extended IFS (EIFS)

- Used by every station when the PHY layer notifies the MAC layer that a transmission has not been correctly received
- Avoids that stations with bad channels disrupt other stations' performance
- Forces fairness in the access is one station does not receive an ACK (e.g. hidden terminal)
- Reduce the priority of the first retransmission (indeed make it equal to all others)
- Set to: DIFS + 1 ACK slot

DCF Access Scheme

Basic Characteristics

- Its implementation is mandatory
- DCF is based on the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) scheme:
  - stations that have data to transmit contend for accessing the channel
  - a station has to repeat the contention procedure every time it has a new data frame to transmit
IEEE 802.11 MAC Protocol
Overview: CSMA/CA

802.11 CSMA: sender
- if sense channel idle for DIFS sec.
  then transmit entire frame (no collision detection)
- if sense channel busy then random access over a contention window CWmin (CA)

802.11 CSMA receiver:
if received OK
return ACK after SIFS

IEEE 802.11 MAC Protocol: others

- NAV: Network Allocation Vector
  - 802.11 frame has transmission time field
  - others (hearing data) defer access for NAV time units
  - NAV is contained in the header of frames
  - Allows reducing energy consumption
  - Helps reducing hidden terminals problems

Hidden Terminal Effect

- hidden terminals: A, C cannot hear each other
  - obstacles, signal attenuation
  - collisions at B
- goal: avoid collisions at B
- CSMA/CA with handshaking
IEEE 802.11 MAC Protocol Overview: Handshaking

- CSMA/CA: explicit channel reservation
  - sender: send short RTS: request to send
  - receiver: reply with short CTS: clear to send
  - CTS reserves channel for sender, notifying (possibly hidden) stations
- avoid hidden station collisions

- RTS and CTS are short:
  - collisions of shorter duration, hence less "costly"
  - the final result is similar to collision detection
- DCF allows:
  - CSMA/CA
  - CSMA/CA with reservations

The DCF Access Scheme

- Basic
  - the simplest scheme
  - used when the data frames to be transmitted have a fairly short duration
- With handshaking
  - Uses additional control frames for channel access
  - Designed to solve the problems of hidden terminals
  - Provides higher reliability in data transmission
The exposed terminal problem

- Sensing range is normally larger than receiving range
- Terminals may be "exposed" in that they sense the channel occupied, but cannot compete for it

DCF
The Basic Access Mode

Carrier Sensing

- Used to determine whether the channel is busy or idle
- Performed at the physical layer (physical carrier sensing) and at the MAC layer (virtual carrier sensing)
  - **Physical carrier sensing**: detection of nearby energy sources
  - **Virtual carrier sensing**: the frame header indicates the remaining duration of the current Channel Access Phase (till ACK is received)
Network Allocation Vector (NAV)

- Used by the stations nearby the transmitter to store the duration of the frame that is occupying the channel.
- The channel will become idle when the NAV expires.
- Upon the NAV expiration, stations that have data to transmit listen to the channel again.

Using DIFS and SIFS

Transmitter:
- senses the channel
- if the channel is idle, it waits a time equal to DIFS
- if the channel remains idle for DIFS, it transmits its MPDU

Receiver:
- computes the checksum thus verifying whether the transmission is correct
- if so, it sends an ACK after a time equal to SIFS
- it should always transmit an ACK with a rate less than or equal to the one used by the transmitter and no larger than 2Mbit/s
Using DIFS and SIFS

• Neighbors:
  - set their NAV to the value indicated in the transmitted MPDU
  - NAV set to: the MPDU tx time + 1 SIFS + ACK time

MPDU Transmission

Frame Retransmissions

• A frame transmission may fail because of collision or errors on the radio channel
• A failed transmission is re-attempted till a max no. of retransmissions is reached
• ARQ scheme: Stop&Wait
Collision Avoidance (CA)

Backoff procedure

- If a station senses the channel busy, it waits for the channel becoming idle
- As soon as the channel is idle for DIFS, the station
  - computes the backoff time interval
  - sets the backoff counter to this value
- The station will be able to transmit when its backoff counter reaches 0

MPDU Transmission

- DATA, SIFS, source
- ACK, destination
- NAV, DIFS, CW, backoff

CW=Contention Window

Backoff Value

- Integer value corresponding to a number of time slots
- The number of slots is a r.v. uniformly distributed in [0,CW-1]
- CW is the Contention Window and at each transmission attempt is updated as:
  - For i=1, CW_i=CW_{min}
  - For i>1, CW_i=2CW_{i-1} with i>1 being the no. of consecutive attempts for transmitting the MPDU
  - For any i, CW_i≤CW_{max}
**Backoff Decrease**

- While the channel is busy, the backoff counter is frozen
- While the channel is idle, and available for transmissions the station decreases the backoff value until
  - the channel becomes busy or
  - the backoff counter reaches 0

**Accessing the Channel**

- If more than one station decrease their counter to 0 at the same time → collision
- Colliding stations have to recompute a new backoff value

**Basic DCF: An Example**

[Diagram of stations A/C and B, showing DIFS, SIFS, and backoff]
Data Fragmentation (1)

- A MSDU is fragmented into more than one frame (MPDU) when its size is larger than a certain fragmentation threshold
  - In the case of failure, less bandwidth is wasted
  - All MPDUs have same size except for the last MPDU that may be smaller than the fragmentation threshold
  - PHY header is inserted in every fragment → convenient if the fragmentation threshold is not too little

Data Fragmentation (2)

- MPDUs originated from the same MSDU are transmitted at distance of SIFS + ACK + SIFS
- The transmitter releases the channel when
  - the transmission of all MPDUs belonging to a MSDU is completed
  - the ACK associated to an MPDU is lost

Data Fragmentation (3)

- Backoff counter is increased for each fragment retransmission belonging to the same frame
- The receiver reassembles the MPDUs into the original MSDU that is then passed to the higher layers
- Broadcast and multicast data units are never fragmented
Recontending for the Channel

- A station recontends for the channel when
  - it has completed the transmission of an MPDU but still has data to transmit
  - a MPDU transmission fails and the MPDU must be retransmitted

- Before recontending the channel after a successful transmission, a station must perform a backoff procedure with CWmin

DCF
Access with handshaking

Access with Handshake

- Used to reserve the channel
- Why?
  - Hidden stations
  - Colliding stations keep transmitting their MPDU; the larger the MPDU involved in the collision, the more bandwidth is wasted
  - Need to avoid collisions, especially when frame is large
  - Particularly useful when a large no. of STAs contend for the channel
**RTS/CTS**

- Handshaking procedure uses the Request to send (RTS) and Clear to send (CTS) control frames.
- RTS / CTS should be always transmitted @1Mbps (they are only headers).
- Access with handshaking is used for frames larger than an RTS_Threshold.

**DCF with Handshaking**

- **Transmitter:**
  - send a RTS (20 bytes long) to the destination
- **Neighbors:**
  - read the duration field in RTS and set their NAV
- **Receiver:**
  - acknowledge the RTS reception after SIFS by sending a CTS (14 bytes long)
- **Neighbors:**
  - read the duration field in CTS and update their NAV
- **Transmitter:**
  - start transmitting upon CTS reception

**MPDU Transmission & NAV**

```
source          destination
    DIFS          SIFS       DATA
    DIFS          SIFS       ACK
    SIFS          SIFS
    SIFS          SIFS
```

```
others
    NAV (RTS)
    NAV (CTS)
    NAV (data)
    DIFS       backoff
```

```
### Basic Characteristics

- Used for services with QoS requirements, it provides a contention-free access to the channel.
- Needs a Point Coordination (PC) that polls the stations → it can be implemented in networks with infrastructure only (AP=PC).
- Stations enabled to operate under the PCF mode are said to be CF-aware (CF=Contention Free).

### PCF

- Stations declare their participation in the CF phase in the Association Request.
- PC builds the polling list based on the received requests.
- Polling list is static.
- Implementation of the polling list and tables are left to the system operator.
Superframe and PCF Protocol

- TBTT: Target Beacon Transmission Time
- D1, D2: frames sent by PC
- U1, U2, U3: frames sent by polled station
- B: beacon frame (sent by AP)
- CFP repetition interval

Examples of frame format

Generic DSSS packet

- SFD – Start Frame Delimiter
- PLPC – Physical Layer Convergence Protocol
- SYNC – 56 bits
- SFD – 16 bits
- SIGNAL – 8 bits
- SERVICE – 8 bits
- LENGTH – 16 bits
- CRC – 16 bits
- PLPC – 1Mbps
- PLPC – 2Mbps
- PSDU – 2, 5.5, 11 Mbps
- 96 μs
### Example: RTS Frame

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration</th>
<th>RA</th>
<th>TA</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Header</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Duration** (in µs): Time required to transmit next (data) frame + CTS + ACK + 3 SIFS
- **RA**: Address of the intended immediate recipient
- **TA**: Address of the station transmitting this frame

### Example: CTS Frame

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration</th>
<th>RA</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Header</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Duration** (in µs): Duration value of previous RTS frame – 1 CTS time – 1 SIFS
- **RA**: The TA field in the RTS frame

### Example: ACK Frame

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration</th>
<th>RA</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Header</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Duration**: set to 0 if More Fragments bit was 0; otherwise equal to the duration of previous frame – 1 ACK – 1 SIFS
- **RA**: copied from the Address 2 field of previous frame
Some Numerical Values...

- **PHY_HDR**: 16 bytes, transmitted @ 1 Mbps
- **MAC_HDR**: 34 bytes, transmitted @ 1 Mbps
  - If slot=20µs, PHY_HDR + MAC_HDR = 20 slots
- **ACK=PHY_HDR+14 bytes, transmitted @ 1 Mbps**
  - If slot=20µs, ACK=12 slots

### Detailed MAC Format (bytes)

<table>
<thead>
<tr>
<th>Field</th>
<th>Bits</th>
<th>Notes/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>15-14</td>
<td>Protocol version. Currently 0</td>
</tr>
<tr>
<td></td>
<td>13-12</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td>11-8</td>
<td>Subtype</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>To DS: 1 = to the distribution system</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>From DS: 1 = exit from the Distribution System</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>More Frag: 1 = more fragment frames to follow (last or unfragmented frame = 0)</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Retry: 1 = this is a re-transmission</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Power Mgt: 1 = station in power save mode, 1 = active mode</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>More Data: 1 = additional frames buffered for the destination address (address x)</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>WEP: 1 = data processed with WEP algorithm, 0 = no WEP</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Order: 1 = frames must be strictly ordered</td>
</tr>
</tbody>
</table>
MAC Format fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Bits</th>
<th>Notes/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration ID</td>
<td>15 - 0</td>
<td>For data frames = duration of frame. For Control Frames the associated identity of the transmitting station.</td>
</tr>
<tr>
<td>Address 1</td>
<td>47 - 0</td>
<td>Source address (6 bytes).</td>
</tr>
<tr>
<td>Address 2</td>
<td>47 - 0</td>
<td>Destination address (6 bytes).</td>
</tr>
<tr>
<td>Address 3</td>
<td>47 - 0</td>
<td>Receiving station address (destination wireless station).</td>
</tr>
<tr>
<td>Sequence Control</td>
<td>15 - 0</td>
<td></td>
</tr>
<tr>
<td>Address 4</td>
<td>47 - 0</td>
<td>Transmitting wireless station.</td>
</tr>
<tr>
<td>Frame Body</td>
<td>0 - 2312 octets (bytes).</td>
<td></td>
</tr>
<tr>
<td>FCS</td>
<td>31 - 0</td>
<td>Frame Check Sequence (32 bit CRC), defined in 802.11.</td>
</tr>
</tbody>
</table>

IEEE 802.11 (Radio) Evolution

<table>
<thead>
<tr>
<th>Standard</th>
<th>802.11b (Wi-Fi)</th>
<th>802.11a</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>83.5 MHz</td>
<td>300 MHz</td>
<td>83.5 MHz</td>
</tr>
<tr>
<td>Frequency of operation</td>
<td>2.4-2.4835 GHz</td>
<td>5.15-5.35 GHz</td>
<td>5.725-5.825 GHz</td>
</tr>
<tr>
<td>Number of non-overlapping channels</td>
<td>3 Indoor/Outdoor</td>
<td>4 Indoor/Outdoor</td>
<td>4 Indoor/Outdoor</td>
</tr>
<tr>
<td>Data rate per channel</td>
<td>1.2, 5.5, 11 Mbps</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
<td>1.2, 5.5, 11 // 6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
</tr>
<tr>
<td>Physical layer</td>
<td>DSSS</td>
<td>OFDM</td>
<td>DSSS // OFDM</td>
</tr>
</tbody>
</table>

802.11g PHY

- Full backward compatibility with 802.11b
- Supports the 802.11b specified data rates of 1, 2, 5.5 and 11 Mbps
- Adds further data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps using OFDM
- Only Tx and Rx of OFDM @ 6, 12 and 24 Mbps is mandatory
- OFDM uses 52 sub-carriers are modulated using BPSK, QPSK, 16-QAM or 64-QAM
- Forward Error Correction (convolutional coding) is used with a coding rate of \( \frac{1}{2} \), 2/3 or \( \frac{3}{4} \)
802.11g PHY

- Improved data rate is paid for with a smaller transmission range
- Improved data rates apply only to the payload: useless with small packets (60-80% of Internet packets are < than 100 bytes!)
- The overall performance is heavily influenced by the "worst channel syndrome"
- 802.11 MAC shares the channel based on access rounds not time