Mobile Communications
Chapter 7: Wireless LANs

- Characteristics
- IEEE 802.11 (PHY, MAC, Roaming, .11a, b, g, h, i, n ... z)
- Bluetooth / IEEE 802.15.x
- IEEE 802.16/.20/.21/.22
- RFID
- Comparison

Prof. Jó Ueyama
Mobile Communication Technology according to IEEE (examples)

**WiFi**
- Local wireless networks
  - **WLAN** 802.11
    - 802.11a → 802.11h
    - 802.11i/e/.../n/.../z
    - 802.11b → 802.11g

**ZigBee**
- Personal wireless nw
  - **WPAN** 802.15
    - 802.15.4 → 802.15.4a/b/c/d/e
    - 802.15.5, .6 (WBAN)
    - 802.15.1
    - 802.15.2
    - 802.15.3 → 802.15.3b/c

**Bluetooth**
- Wireless distribution networks
  - **WMAN** 802.16 (Broadband Wireless Access)
  - **WiMAX**
    - + Mobility
      - [802.20 (Mobile Broadband Wireless Access)]
      - 802.16e (addition to .16 for mobile devices)
Main features of the existing wireless technologies

- 200 Mbps: 802.11n
- 54 Mbps: 802.11a,g
- 5–11 Mbps: 802.11b
- 4 Mbps: UMTS/WCDMA-HSDPA, CDMA2000-1xEVDO
- 1 Mbps: 802.15.1
- 384 Kbps: UMTS/WCDMA, CDMA2000
- 56 Kbps: IS-95, CDMA, GSM

Distance:
- Interna: 10–30m
- Externa: 50–200m
- Externa de meia distância: 200m–4km
- Externa de longa distância: 5km–20km
Characteristics of wireless LANs

- **Advantages**
  - very flexible within the reception area
  - Ad-hoc networks without previous planning possible
  - (almost) no wiring difficulties (e.g. historic buildings, firewalls)
  - more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

- **Disadvantages**
  - typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium
  - many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11n)
  - products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000
Design goals for wireless LANs

- global, seamless operation
- low power for battery use (e.g. WSNs and cell phones)
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks (i.e. interoperable with wired LANs)
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary
Comparison: infrared vs. radio transmission

- **Infrared**
  - uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)

- **Advantages**
  - simple, cheap, available in many mobile devices
  - no licenses needed
  - simple shielding possible

- **Disadvantages**
  - interference by sunlight, heat sources etc.
  - many things shield or absorb IR light
  - low bandwidth

- **Example**
  - IrDA (Infrared Data Association) interface available everywhere

- **Radio**
  - typically using the license free ISM band at 2.4 GHz

- **Advantages**
  - experience from wireless WAN and mobile phones can be used
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)

- **Disadvantages**
  - very limited license free frequency bands
  - shielding more difficult, interference with other electrical devices

- **Example**
  - Many different products
Comparison: infrastructure vs. ad-hoc networks

infrastructure network

ad-hoc network

AP: Access Point
802.11 - Architecture of an infrastructure network

- **Station (STA)**
  - terminal with access mechanisms to the wireless medium and radio contact to the access point

- **Basic Service Set (BSS)**
  - group of stations using the same radio frequency

- **Access Point**
  - station integrated into the wireless LAN and the distribution system

- **Portal**
  - bridge to other (wired) networks

- **Distribution System**
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

![Diagram of 802.11 LAN network components: STA, BSS, Access Point, Portal, Distribution System.](image)
802.11 - Architecture of an ad-hoc network

- Direct communication within a limited range
- Station (STA): terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS): group of stations using the same radio frequency
IEEE standard 802.11

- Mobile terminal
- Access point
- Infrastructure network

**Logical Link Control (LLC)**: Interface between different medias

<table>
<thead>
<tr>
<th>Application</th>
<th>802.11 MAC</th>
<th>802.3 MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>802.11 PHY</td>
<td>802.3 PHY</td>
</tr>
<tr>
<td>IP</td>
<td>802.11 PHY</td>
<td>802.3 PHY</td>
</tr>
</tbody>
</table>

**802.11 PHY**

**802.3 PHY**

**802.11 MAC**

**802.3 MAC**
802.11 - Layers and functions

- **MAC**
  - access mechanisms, fragmentation, encryption
- **MAC Management**
  - synchronization, roaming, MIB, power management

**PHY Management includes**
- **PLCP** Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- **PMD** Physical Medium Dependent
  - modulation, coding, transforms bits into signals

- **Station Management**
  - coordination of all management functions
802.11 - Physical layer (legacy)

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading
  - Frequency multiplexing
- DSSS (Direct Sequence Spread Spectrum)
  - Multiplexes by code (i.e. using a chipping code)
  - Implementation is more complex than FHHS
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, -1, -1, -1 (Barker code)
  - DATA XOR chipping code
- Infrared
  - Wavelength around 850-950 nm, diffuse light, typ. 10 m range
  - uses near visible light
  - carrier detection, up to 4Mbits/s data rate
FHSS PHY packet format (legacy)

- **Synchronization**
  - synch with 010101... pattern

- **SFD (Start Frame Delimiter)**
  - 0000110010111101 start pattern

- **PLW (PLCP_PDU Length Word)**
  - length of payload incl. 32 bit CRC of payload, PLW < 4096

- **PSF (PLCP Signaling Field)**
  - data rate of the payload (0000 -> the lowest data rate)

- **HEC (Header Error Check)**
  - checksum with the standard ITU-T polynomial generator

![Diagram of FHSS PHY packet format](image-url)
DSSS PHY packet format (legacy)

- **Synchronization**
  - synch., gain setting, energy detection, frequency offset compensation
- **SFD (Start Frame Delimiter)**
  - 1111001110100000
- **Signal**
  - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- **Service**
  - future use, 00: 802.11 compliant
- **Length**
  - length of the payload
- **HEC (Header Error Check)**
  - protected by checksum using ITU-T standard polynomial error check

![PLCP preamble and header diagram](image)
802.11 - MAC layer I - DFWMAC

- MAC layer has to fulfill several tasks including:
  - control medium access
  - support for roaming
  - authentication
  - power conservation

- In summary, it has two key tasks:
  - traffic services
  - access control
Traffic services (two implementations)
- Asynchronous Data Service (mandatory)
  - exchange of data packets based on "best-effort"
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

Access methods
- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized "back-off" mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list
Priorities
- defined through different inter frame spaces
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF Inter frame spacing)
  - lowest priority, for asynchronous data service
802.11 - CSMA/CA access method I

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)
802.11 - competing stations - simple version

- busy: medium not idle (frame, ack etc.)
- \( bo_e \): elapsed backoff time
- \( bo_r \): residual backoff time
- \( \downarrow \): packet arrival at MAC

Diagram:

- Station 1
  - DIFS
  - Busy
  - \( bo_e \) for \( bo_r \)

- Station 2
  - Busy
  - \( bo_e \) for \( bo_r \)

- Station 3
  - Busy

- Station 4
  - Busy
  - \( bo_e \) for \( bo_r \)

- Station 5
  - Busy
  - \( bo_e \) for \( bo_r \)

Diagram shows the timing and state transitions of competing stations in a simple 802.11 network scenario.
802.11 - CSMA/CA access method II

- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors
802.11 - DFWMAC

- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement via ACK
  - other stations store medium reservations distributed via RTS and CTS
Fragmentation

- **DIFS**
- **RTS**
- **SIFS**
- **CTS**
- **SIFS**
- **ACK**
- **SIFS**
- **DIFS**

**sender**
- RTS
- **SIFS**
- CTS
- **SIFS**
- **ACK**
- **SIFS**
- **ACK**
- **SIFS**

**receiver**
- NAV (RTS)
- NAV (CTS)
- NAV (frag1)
- NAV (ACK1)
- NAV (ACK2)
- **SIFS**

**other stations**
- NAV (frag1)
- NAV (ACK1)
- NAV (ACK2)

**t**
- data

**contention**
DFWMAC-PCF I (almost never used)

D – downstream data
U – upstream data
DFWMAC-PCF II

D – downstream data
U – upstream data

point coordinator
wireless stations
stations’ NAV

contention free period
contention period

D_3 PIFS D_4 SIFS U_4 CF_{end}
802.11 - Frame format

- **Types**
  - control, management (e.g., beacon) and data frames
- **Sequence numbers**
  - important against duplicated frames due to lost ACKs
- **Addresses**
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- **Miscellaneous**
  - sending time, checksum, frame control, data

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Frame Control</th>
<th>Duration/ID</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Sequence Control</th>
<th>Address 4</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bits</th>
<th>Protocol version</th>
<th>Type</th>
<th>Subtype</th>
<th>To DS</th>
<th>From DS</th>
<th>More Frag</th>
<th>Retry</th>
<th>Power Mgmt</th>
<th>More Data</th>
<th>WEP</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
## MAC address format

<table>
<thead>
<tr>
<th>scenario</th>
<th>to DS</th>
<th>from DS</th>
<th>address 1</th>
<th>address 2</th>
<th>address 3</th>
<th>address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad-hoc network</td>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, from AP</td>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, to AP</td>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, within DS</td>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

DS: Distribution System  
AP: Access Point  
DA: Destination Address  
SA: Source Address  
BSSID: Basic Service Set Identifier  
RA: Receiver Address  
TA: Transmitter Address  
Address1 – destination  
Address2 – source (ACK will be sent to)  
Address3 – filter (often it will carry BSSID addr)  
Address4 – Address of the source Access Point
### Special Frames: ACK, RTS, CTS

#### Acknowledgement

- **ACK**
  - Frame Control: 2 bytes
  - Duration: 2 bytes
  - Receiver Address: 6 bytes
  - CRC: 4 bytes

#### Request To Send

- **RTS**
  - Frame Control: 2 bytes
  - Duration: 2 bytes
  - Receiver Address: 6 bytes
  - Transmitter Address: 6 bytes
  - CRC: 4 bytes

#### Clear To Send

- **CTS**
  - Frame Control: 2 bytes
  - Duration: 2 bytes
  - Receiver Address: 6 bytes
  - CRC: 4 bytes
802.11 - MAC management

- **Synchronization**
  - try to find a LAN, try to stay within a LAN
  - timer etc.

- **Power management**
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements

- **Association/Reassociation**
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network

- **MIB - Management Information Base**
  - managing, read, write
Synchronization using a Beacon (infrastructure)

beacon interval (20ms – 1s)

access point medium

value of the timestamp

beacon frame
Synchronization using a Beacon (ad-hoc)

- Beacon interval
- Station 1: $B_1$
- Station 2: $B_2$
- Medium: busy
- Value of the timestamp
- Beacon frame
- Random delay
Power management

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)
- APSD (Automatic Power Save Delivery)
  - new method in 802.11e replacing above schemes
Power saving with wake-up patterns (infrastructure)

TIM interval

DTIM interval

access point

medium

station

T TIM

D DTIM

B broadcast/multicast

p PS poll

d data transmission to/from the station

busy

awake

data transmission to/from the station

7.32
Power saving with wake-up patterns (ad-hoc)

- **Station 1**
  - $B_1$ beacon frame
  - Random delay
  - $A$ transmit ATIM
  - $D$ transmit data
  - Awake

- **Station 2**
  - $B_2$ beacon frame
  - $a$ acknowledge ATIM
  - $d$ acknowledge data

**Diagram Details**
- ATIM window
- Beacon interval

**Legend**
- B beacon frame
- awake
- a acknowledge ATIM
- d acknowledge data
802.11 - Roaming

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources
- Fast roaming – 802.11r
  - e.g. for vehicle-to-roadside networks
WLAN: IEEE 802.11b

- **Data rate**
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s

- **Transmission range**
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor

- **Frequency**
  - DSSS, 2.4 GHz ISM-band

- **Security**
  - Limited, WEP insecure, SSID

- **Availability**
  - Many products, many vendors

- **Connection set-up time**
  - Connectionless/always on

- **Quality of Service**
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)

- **Manageability**
  - Limited (no automated key distribution, sym. Encryption)

- **Special Advantages/Disadvantages**
  - Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only
IEEE 802.11b – PHY frame formats

Long PLCP PPDU format

- **synchronization**: 128 bits
- **SFD**: 16 bits
- **signal**: 8 bits
- **service**: 8 bits
- **length**: 16 bits
- **HEC**: 16 bits
- **payload**: variable bits

PLCP preamble

- 192 µs at 1 Mbit/s DBPSK

PLCP header

- 1, 2, 5.5 or 11 Mbit/s

Short PLCP PPDU format (optional)

- **short synch.**: 56 bits
- **SFD**: 16 bits
- **signal**: 8 bits
- **service**: 8 bits
- **length**: 16 bits
- **HEC**: 16 bits
- **payload**: variable bits

PLCP preamble

- (1 Mbit/s, DBPSK)
  - 96 µs

PLCP header

- (2 Mbit/s, DQPSK)
  - 2, 5.5 or 11 Mbit/s
Channel selection (non-overlapping)

Europe (ETSI)

- Channel 1: 2400 MHz to 2412 MHz
- Channel 7: 2442 MHz to 2454 MHz
- Channel 13: 2472 MHz to 2483.5 MHz

US (FCC)/Canada (IC)

- Channel 1: 2400 MHz to 2412 MHz
- Channel 6: 2437 MHz to 2449 MHz
- Channel 11: 2462 MHz to 2474 MHz

Frequency range: 22 MHz
WLAN: IEEE 802.11a

- **Data rate**
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory

- **Transmission range**
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30 m, 18 up to 40 m, 12 up to 60 m

- **Frequency**
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band

- **Security**
  - Limited, WEP insecure, SSID

- **Availability**
  - Some products, some vendors

- **Connection set-up time**
  - Connectionless/always on

- **Quality of Service**
  - Typ. best effort, no guarantees (same as all 802.11 products)

- **Manageability**
  - Limited (no automated key distribution, sym. Encryption)

- **Special Advantages/Disadvantages**
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, no QoS
IEEE 802.11a – PHY frame format

- **PLCP preamble**
- **signal**
- **data**

**PLCP header**

- Rate (4 bits)
- Reserved (1 bit)
- Length (12 bits)
- Parity (1 bit)
- Tail (6 bits)
- Service (16 variable bits)
- Payload (6 variable bits)
- Tail (1 bit)
- Pad (variable bits)

**Symbols**

- 6 Mbit/s
- 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
Operating channels of 802.11a in Europe

Center frequency = 5000 + 5*channel number [MHz]
Operating channels for 802.11a / US
U-NII

channel

center frequency = 5000 + 5*channel number [MHz]
OFDM in IEEE 802.11a

- OFDM with 52 used subcarriers (64 in total)
  - 48 data + 4 pilot
    - (plus 12 virtual subcarriers)
  - 312.5 kHz spacing