Overview of IEEE 802.11b Wireless LAN

S-72.4210 Postgraduate course in Radio Communications

10.1.2006

Tommi Koivisto

tommi.koivisto@tkk.fi

Outline

- Introduction
- Standardization
- Physical layer (PHY)
  - Direct-sequence spread spectrum
  - Complementary Code Keying
  - Physical layer convergence protocol (PLCP)
- Medium access control layer (MAC)
  - CSMA/CA
  - MAC frames
- Conclusion
- References
- Homework

Introduction

- IEEE 802.11b is a wireless LAN standard that defines a physical layer and MAC layer for wireless communications within a short range (up to 300 meters) and with low power consumption.
- IEEE 802.11b provides a substitute for wired LAN and also offers flexibility in terms of mobility.
- The 802.11b is an extension for the original 802.11 and provides up to 11 Mbps transmission rates over the air interface.
- Devices have been on the market for several years now. Currently the dominating WLAN standard seems to be 802.11g, but most of those devices are compatible also with 802.11b.
- WLAN networks can be either infrastructured networks, when there is an access point (AP) that controls access to the (wired) network, or ad hoc networks that are composed solely of the stations transmitting to each other.

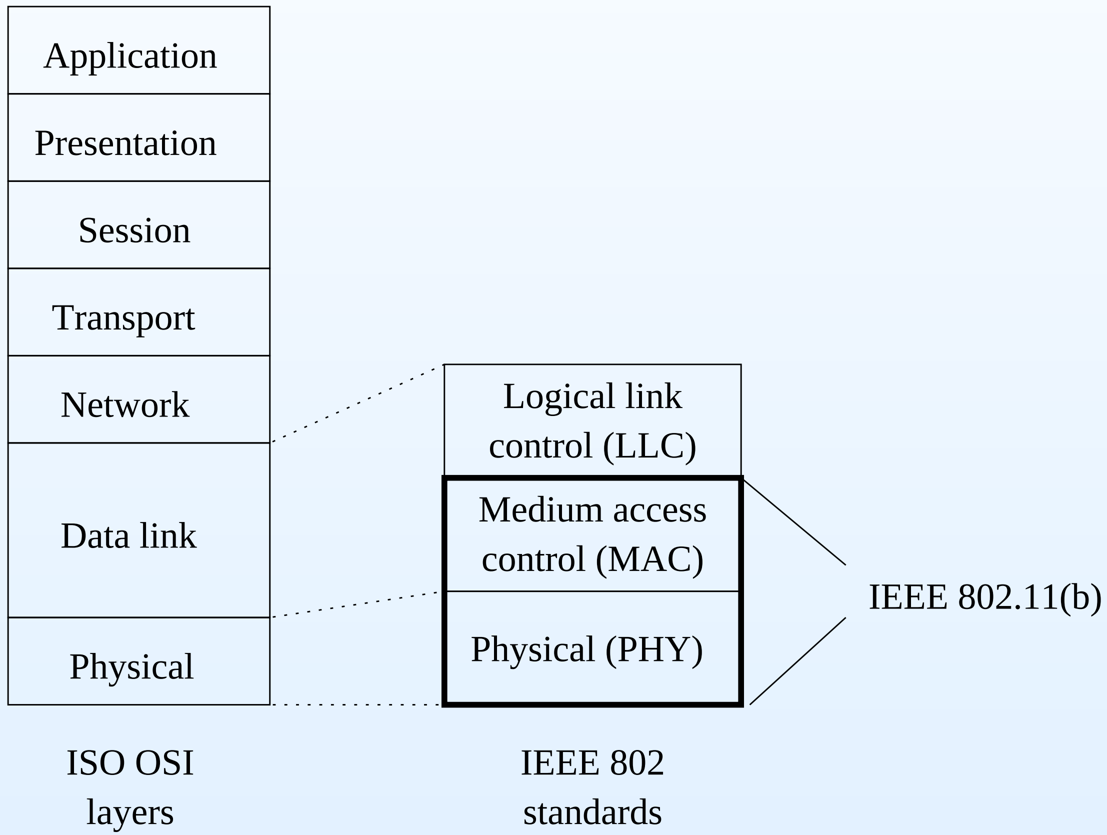
IEEE 802.11 standards

- **IEEE 802.11: up to 2 Mbps, 2.4 GHz, approved in 1997**
- IEEE 802.11a: up to 54 Mbps, 5 GHz, approved in 1999
- **IEEE 802.11b: up to 11 Mbps, 2.4 GHz, approved in 1999**
- IEEE 802.11g: up to 54 Mbps, 2.4 GHz, approved in 2003
- IEEE 802.11e: new coordination function for QoS, not yet approved
- IEEE 802.11f: IAPP, inter-AP protocol, approved in 2003
- IEEE 802.11h: use of 5 GHz band in Europe, approved in 2003
- IEEE 802.11i: new encryption standards, approved in 2004
- IEEE 802.11n: MIMO physical layer, not yet approved

Standards are available at http://standards.ieee.org/getieee802/portfolio.html

IEEE 802.11 standards

IEEE 802.11 standards specify MAC and PHY layers. PHY layer is further divided into PLCP (physical layer convergence procedure) and PMD (physical medium dependent) sublayers.

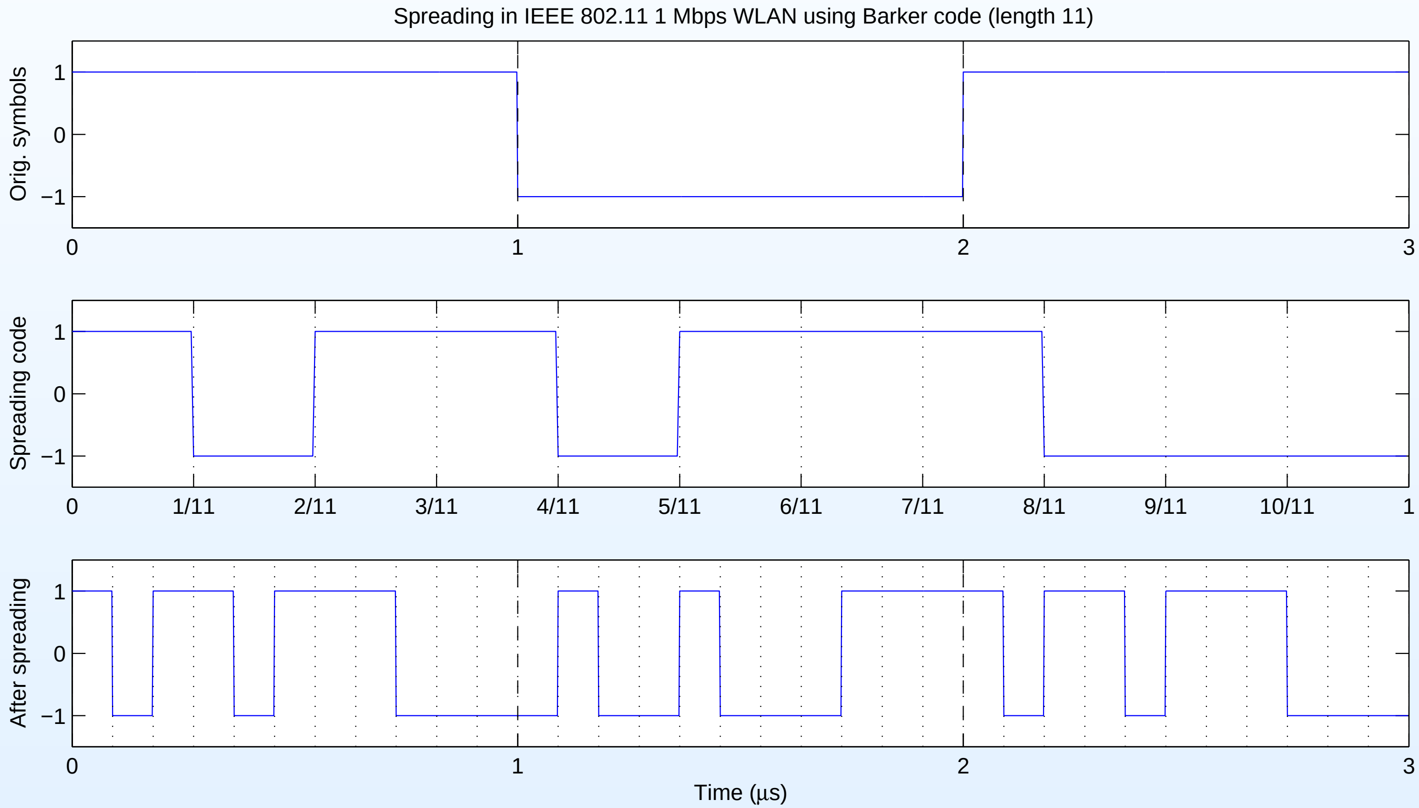


Physical layer

- IEEE 802.11b WLAN operates at the ISM frequency band which is 2.4 GHz - 2.4835 GHz in USA and Europe and 2.471-2.497 GHz in Japan.
- The frequency band is divided into 14 partially overlapping channels each 22 MHz wide. In Europe, 13 of these are available, 11 in USA and only one in Japan.
- All devices within the same BSS (basic service set) use the same channel.
- The chip rate over the radio interface is 11 MHz. Supported transmission rates in are 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps.
- 1 Mbps and 2 Mbps rates are obtained using direct-sequence spread spectrum (DSSS) as specified in IEEE 802.11.
- 5.5 Mbps and 11 Mbps rate are obtained using complementary code keying (CCK) modulation.

Direct-sequence spread spectrum

- In DSSS, the transmitted signal is spread in bandwidth using a spreading code. Each symbol is multiplied by the spreading code:



Direct-sequence spread spectrum

- Since the chip rate after spreading is faster than the symbol rate, the bandwidth is increased (by a factor that equals the length of the spreading code).
- At the receiver, the signal is despread by a filter that is matched to the spreading code.
- This reduces interference and introduces processing gain to the desired signal.
- The amount of processing gain is calculated as

$$G = \frac{\text{Chip rate}}{\text{Symbol rate}}$$

- Thus, DSSS tolerates interference well which is especially important when operating at the ISM band.

DSSS-based PHY

- The DSSS-based PHY specified in IEEE 802.11 can be used for data rates of 1 Mbps and 2 Mbps.
- The used spreading code is an 11-chip Barker sequence +1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1.
- Barker sequence has very good autocorrelation properties and is thus ideal for environments with interference.
- The processing gain for a code of length 11 is 10.4 dB.
- In 1 Mbps PHY, differential BPSK is used as modulation method after spreading.
- In 2 Mbps PHY, differential QPSK is used (the same code is used in both I- and Q-branches).
- IEEE 802.11b devices support also DSSS-based PHY.

Complementary Code Keying

- IEEE 802.11b defines PHY layer for higher data rates 5.5 Mbps and 11 Mbps. This is called HR/DSSS for high rate/DSSS.
- In HR/DSSS, complementary code keying is used as a modulation method.
- CCK is an M-ary orthogonal keying modulation method where one of the M unique (almost orthogonal) signal code words are chosen for transmission.
- The length of a code word is 8 => the duration of one symbol is 8 complex chips. The chip rate is still 11 MHz, so the radio parts of the transmitter stay the same as in 802.11.

Complementary Code Keying

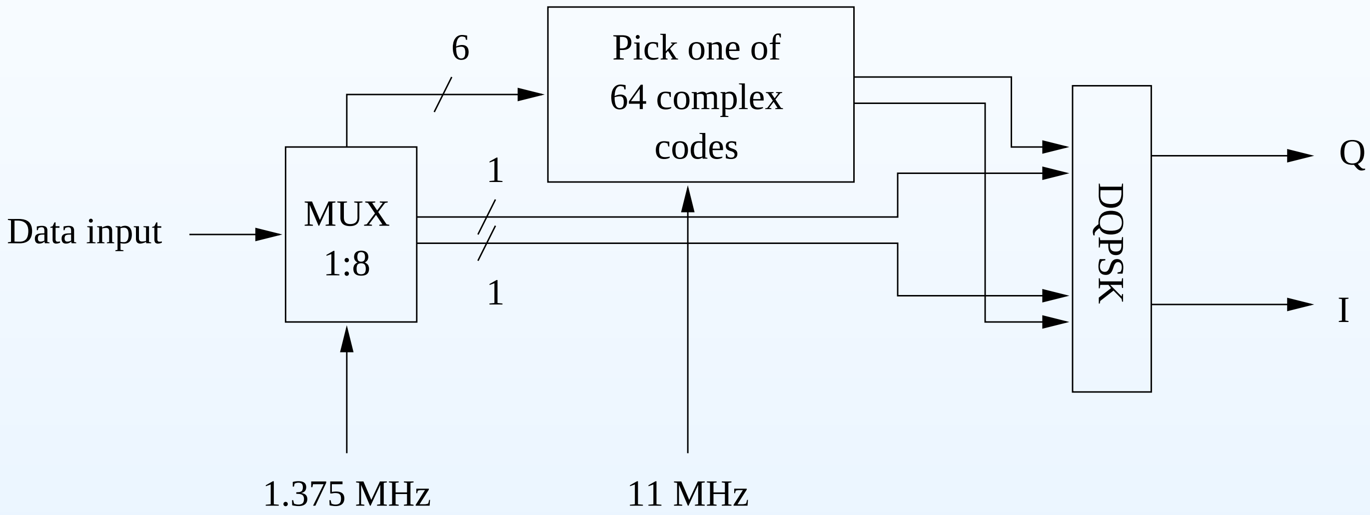
- The 8-chip code words are defined in both case of 5.5 Mbps and 11 Mbps as

$$\mathbf{c} = \Big[e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)}, -e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_1}\Big]$$

- The first two bits b_0 and b_1 encode ϕ_1 based on DQPSK, i.e. the phase ϕ_1 is relative to the phase ϕ_1 in the previous symbol.
- In case of 11 Mbps, bits b_2-b_7 encode ϕ_2,ϕ_3 and ϕ_4 in the same way based on DQPSK.
- In case of 5.5 Mbps, only 4 bits are transmitted during one code period. The codeword set is a subset of the codewords used in 11 Mbps mode, so same hardware can be used for generating them.

Complementary Code Keying

- Only six bits need to be fed to the code generation block, since the first two bits (ϕ_1) affect all chips:

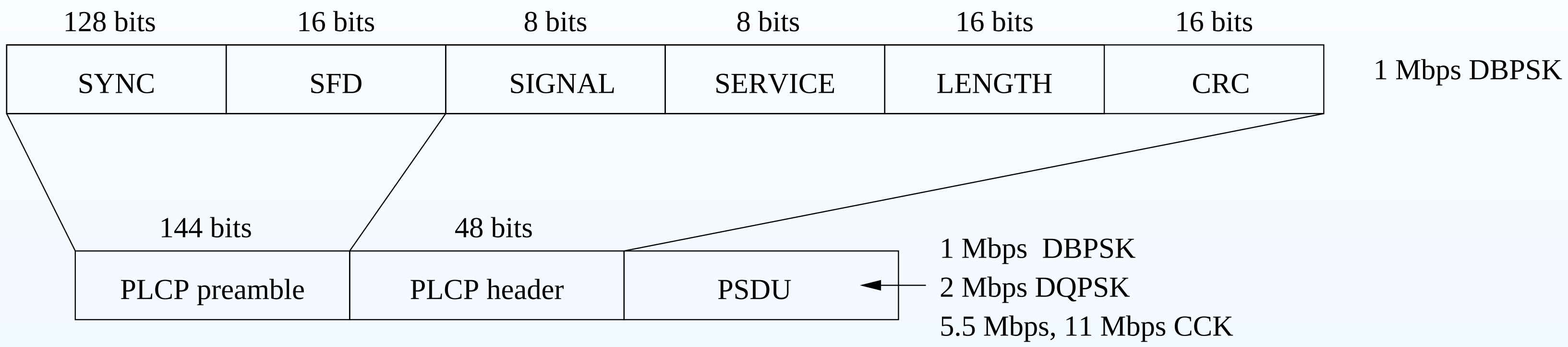


- At the receiver, the transmitted bits are detected by finding the correct codeword using a bank of 64 correlators. Also, phase detection for the code that gave the largest correlator output is needed.

Physical layer convergence protocol

- Physical layer convergence protocol defines a method of mapping the MAC layer data units into frames suitable for transmitting and receiving across the air interface.
- IEEE 802.11b specifies two different PLCP preambles and headers: the long PLCP preamble and header that are mandatory and an optional short preamble and header that can be used in order to get maximum data throughput.
- The preamble and header are always carried using 1 Mbps DBSPK mode. The header determines the transmission rate for the service data units (the actual data).

Long PLCP frames



- PLCP frames contain a preamble, a header and the carried data (PSDU).
- The preamble consists of
  - A 128-bit SYNC field that consists of scrambled "1" bits and is used for synchronization.
  - A 16-bit SFD field that only indicates the start of PHY-dependent parameters.

Long PLCP frames

- The header consists of
  - An 8-bit SIGNAL field that indicates the transmission rate (modulation) that is used for carrying the data units.
  - An 8-bit SERVICE field that is mostly reserved for future use.
  - A 16-bit LENGTH field that indicates the length of the PSDU.
  - A 16-bit CRC check that is calculated for the SIGNAL,SERVICE and LENGTH fields.
- The PSDU field carries the MAC frames.

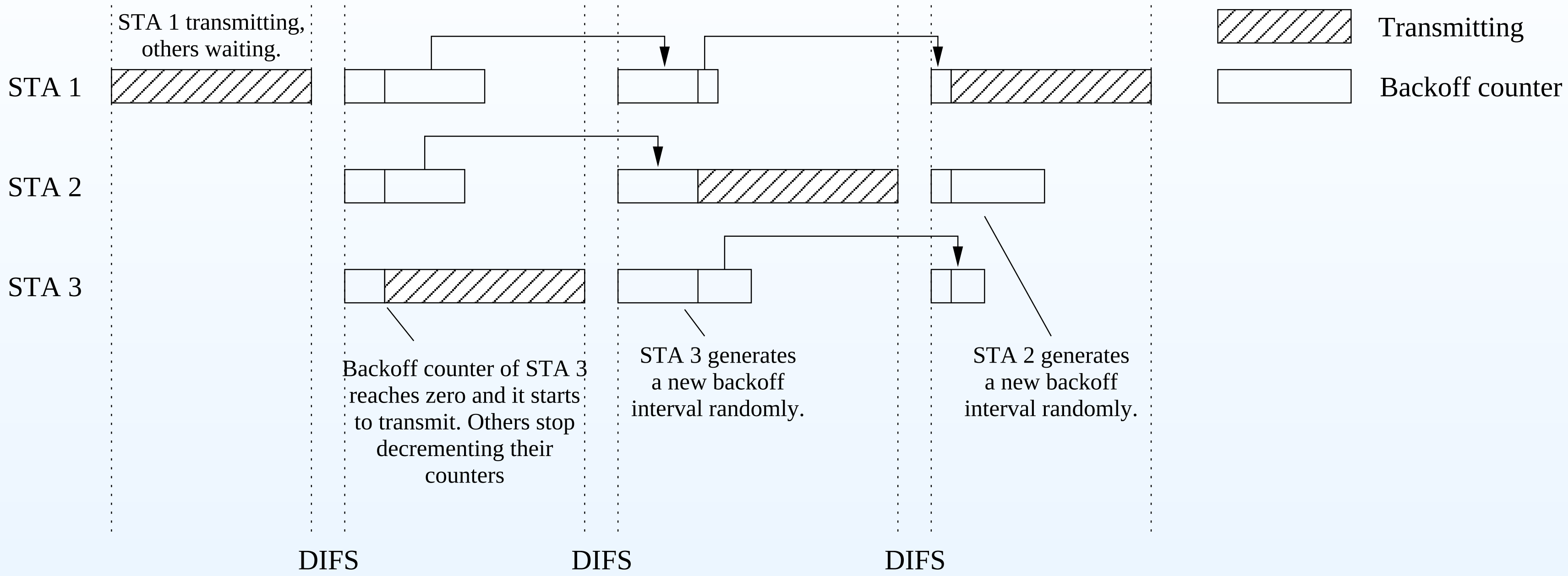
Medium access control layer

- Medium access control (MAC) layer controls the access of the stations to the medium (radio interface).
- In IEEE 802.11(b), the access to the medium is controlled through *coordination functions*:
  - Distributed coordination function (DCF): All stations participate in the medium access control using CSMA/CA access scheme.
  - Point coordination function (PCF): An access point controls the medium access by polling the stations periodically. This is an optional feature that is not very widely implemented.
- DCF provides contention-based access whereas PCF can be used to provide contention-free services.
- MAC layer also handles ARQ, addressing and authentication, among others.

CSMA/CA

- The basic multiple access scheme used in IEEE 802.11(b) is a DCF called *carrier sense multiple access with collision avoidance* (CSMA/CA).
- Before a station starts to transmit, it senses the medium to determine if another station is transmitting:
  - If the medium is idle for a duration >= distributed interframe spacing (DIFS), the station starts transmitting.
  - If the medium is busy, the station shall do the following:
    1. Wait until the end of current transmission.
    2. After the medium has been idle for a duration of DIFS, the station selects a random backoff interval counter and starts decrementing it while the medium is idle.
    3. After the counter reaches zero, the station starts transmitting.
    4. If the medium becomes busy while decrementing the counter, the counter is stopped until the medium becomes idle again.

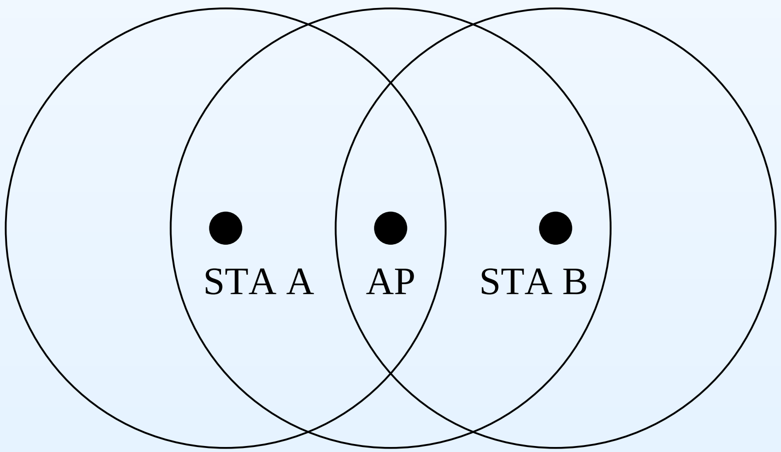
CSMA/CA



Obviously, as the number of transmitting stations increases, the throughput of a single station decreases rapidly.

Hidden node problem

- The hidden node problem occurs when there are two stations A and B that can not hear each other both trying to send to the same access point AP (or any other station).
- Both A and B sense that the medium is idle and start transmitting. They can not hear each other, but AP hears both of them, so collision will occur at AP.



Station A is hidden from station B

RTS/CTS

- To get around the hidden node problem, a refinement to the distributed coordination function has been specified.
- The problem is solved using a RTS (request to send) / CTS (clear to send) protocol prior to packet transmission.
- The station A that wants to transmit first sends an RTS packet to the receiving station AP. The receiving station AP then responds with a CTS packet if the medium is idle.
- Other station B that can not hear the RTS packet, can hear the CTS packet coming from AP and will thus defer the transmission.
- RTS and CTS packets are very short, so it is less probable that they will collide with RTS packets of other stations.

Point coordination function

- Point coordination is an optional feature that offers contention-free service (i.e. no collisions).
- Point coordination is used only in an infrastructured network topology. The point coordinator is then the access point.
- The AP uses a round-robin policy to poll each station for data to be transmitted.
- If PCF is implemented, it co-exists with DCF so that PCF and DCF alternate, thus creating a contention-free period followed by contention period.
- It is optional for stations to respond to the polls. Those stations that do respond are called CF-pollable.

MAC frame format

Octets:	2	2	6	6	6	2	6	0–2312	4
	Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC header

The MAC frame consists of:

- MAC header, which comprises frame control, duration, address and sequence control information.
- Frame body, which can be 0-2312 octets long.
- A frame check sequence that contains a 32-bit cyclic redundancy code (CRC).

MAC frame format

- In the MAC header, the frame control field controls e.g. frame type, fragmentation, power management and WEP (wired equivalent privacy).
- There are four address fields, not all of which are necessarily present. They are used for transmitter address, receiver address, source address and destination address.
- The sequence control field is used for frame and fragment numbering.

Conclusion

- IEEE 802.11b extends the IEEE 802.11 WLAN standard by providing higher data rates of 5.5 Mbps and 11 Mbps.
- The key technology enabling this is CCK modulation, in which the data bits determine a code word that is transmitted over the air interface. At the receiver, the received codeword is compared to possible codewords by calculating correlation between them.
- At the PLCP layer, the most visible change to 802.11 is the addition of an optional short preamble that enables maximum data throughput.
- MAC layer has not been changed since IEEE 802.11.
- IEEE 802.11b devices are fully compatible with IEEE 802.11 and thus support also 1 Mbps and 2 Mbps rates.

References

[1] IEEE Std 802.11, "Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2003, 528 pages, available at http://standards.ieee.org/getieee802/portfolio.html

[2] IEEE Std 802.11b, "Supplement to Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band", 2003, 96 pages, available at http://standards.ieee.org/getieee802/portfolio.html

References

[3] E. Ferro and F. Potortì, "Bluetooth and Wi-Fi Wireless Protocols: A Survey and a Comparison", IEEE Wireless Communications, vol. 12, no. 1, Feb. 2005, pp. 12–26

[4] R. Jordan and C. T. Abdallah, "Wireless Communications and Networking: An Overview", IEEE Antennas and Propagation Magazine, vol. 44, no. 1, Feb. 2002, pp. 185–193

Homework

1) Explain the basic principles of CCK modulation and demodulation in 11 Mbps mode.

2) 8 bits are transmitted using 11 Mbps mode. Find the I- and Q-branch signals at the output of the modulator when the transmitted bits are 10 11 01 01. You can use the following table to map the bits to DQPSK symbols:

Bits $d_i d_{i+1}$	Phase	Bits $d_i d_{i+1}$	Phase
00	0	01	$\pi/2$
10	π	11	$3\pi/2$

3) Direct-sequence spread spectrum techniques are used for signal transmission and usually DSSS techniques enable CDMA. Give your thoughts on why CDMA is not in the case of IEEE 802.11/11b signals well suitable to be used as a multiple access technique.