Appendix 6

IEEE 802.11: Wireless Local Area Networks (WLANs)

The IEEE 802.11 standard specifies a *wireless local area network (WLAN)* system comprising of a *medium access control (MAC)* protocol and three alternative physical medium implementations. An IEEE 802.11 WLAN is intended to be used as a *physical layer* in conjunction with the IEEE 802.2 *logical link control (LLC)* protocol. Given that the MAC protocol is based on *CSMA/CA (collision sense multiple access with collision avoidance)*, an IEEE 802.11 WLAN is, in effect, a 'wireless ethernet' (Figure A6.1).

WLAN network architecture

A simple 802.11 WLAN comprises a number of *stations* which may operate in one of the following two configurations:

- *independent configuration (basic service set — BSS)* — in this mode, stations communicate directly with one other. There is no formal network structure and such networks are sometimes referred to as *ad hoc networks*. Ad hoc networks are relatively easy to operate, but their coverage area is limited. Such a configuration is termed a *basic service set (BSS).* Where the BSS is not otherwise connected to an external network it is termed an *independent BSS (IBSS).*
- *infra-structure configuration (extended service set — ESS)* — in this configuration, stations select a nearby *access point (AP)* and *associate* with it. The access point (AP) provides access to an external data network, which in IEEE 802.11-terminology is a *distribution system*. Typically most traffic within a given BSS will thus flow via the access point (AP). A number of BSSs can be grouped together to create an *extended service set (ESS).* An ESS is intended to provide for wider WLAN coverage area — by allowing stations to *roam* from one BSS or AP area to another. This is achieved by bridging the separate BSSs across the distribution system.

Figure A6.2 illustrates the station, the basic service set (BSS), the access point (AP) and the *distribution system* of an IEEE 802.11 wireless LAN (WLAN).

Data Networks, IP and the Internet: Protocols, Design and Operation Martin P. Clark
 ISBN: 0-470-84856-1

datalink layer (OSI layer 2)	logical link control (LLC)	IEEE 802.2		
	medium access control (MAC)	IEEE 802.11 (MAC & PLCP)		
physical layer (OSI layer 1)	physical layer convergence protocol (PLCP)			
	physical protocol layer (PHY)	IEEE 802.11 FH-PHY	IEEE 802.11 DS-PHY	IEEE 802.11 IR-PHY

Legend
DS-PHY = direct sequence spread spectrum physical layer
FH-PHY = frequency hopping spread spectrum physical layer
IR-PHY = infra-red physical layer

Figure A6.1 IEEE 802.11 wireless local area network (WLAN): protocol stack.

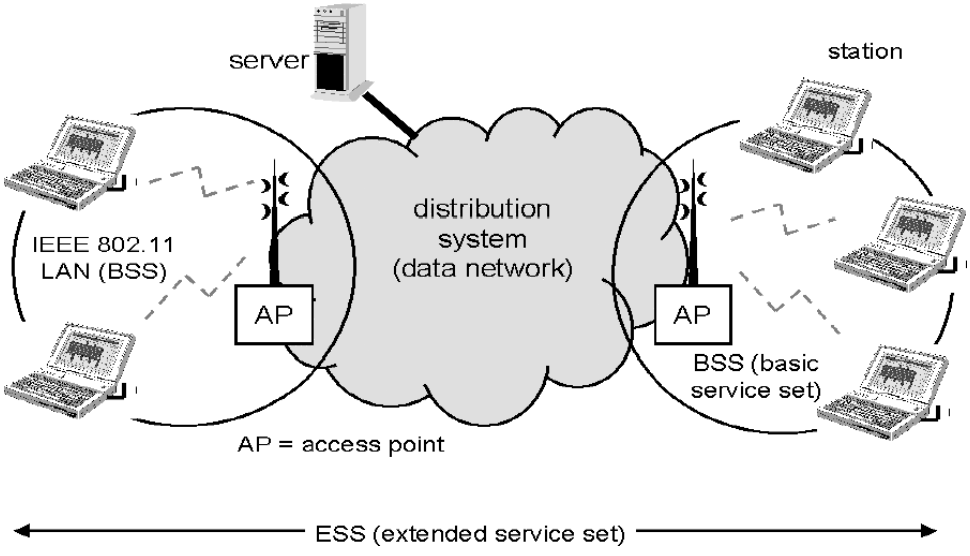


Figure A6.2 IEEE 802.11 wireless local area network (WLAN) architecture.

IEEE 802.11 Specifications

IEEE 802.11 MAC (medium access control) protocol

The MAC protocol is based upon a similar principle of *carrier sense multiple access with collision avoidance (CSMA/CA)* as ethernet LANs (IEEE 802.3). It provides for the following types of *time-bounded services, security services* and *management services*:

- authentication (station service);
- deauthentication (station service);

Table A6.1 IEEE 802.11 wireless local area network (WLAN) specifications

Standard	Contents
802.11	Wireless local area network (WLAN) MAC (medium access control) and PHY (physical layer) specification
802.11a	High speed physical layer in 5 GHz radio band
802.11b	High speed physical layer extension in the 2.4 GHz radio band
802.11c	MAC bridges
802.11d	Specification for operation in additional regulatory domains
802.11e	MAC quality-of-service (QOS) enhancements
802.11f	Multi-vendor access point (AP) interoperability via the Inter-Access-Point protocol (IAPP)
802.11g	Further higher rate data extension in the 2.4 GHz band
802.11h	Transmit power management for use in the 5 GHz band in Europe
802.11i	MAC security enhancements

- privacy (station service);
- MSDU (MAC service data unit) delivery (station service);
- association (distribution system service);
- disassociation (distribution system service);
- distribution (distribution system service);
- integration (distribution system service); and
- reassociation (distribution system service).

MAC frames may be either control frames, management frames or data frames. The format of MAC frames is as shown in Figure A6.3. The various address fields contain different addresses as indicated by the *to DS (destination station)* and *from DS (destination station)* bits (see Table A6.2).

The *power management bit* (when set to value '1') indicates that the power management protocol is in use — for saving battery life by turning off the radio transmitter when not required.

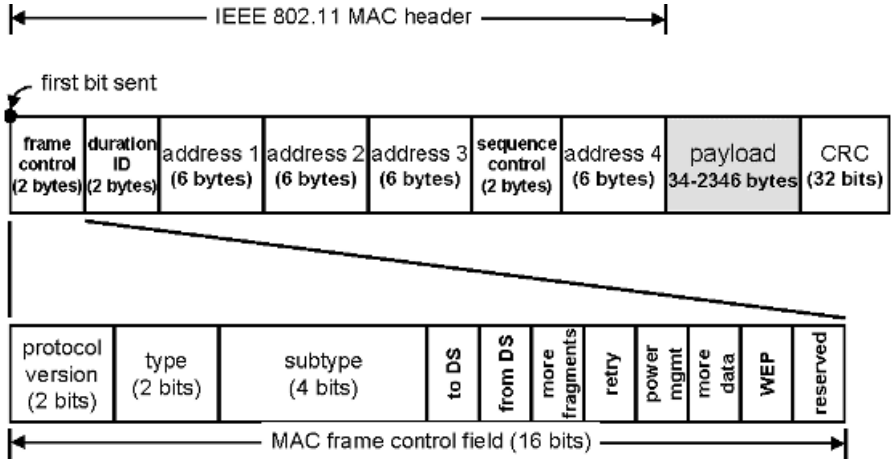


Figure A6.3 IEEE 802.11 MAC (medium access control) protocol frame format.

Table A6.2 IEEE 802.11 MAC (medium access control): use of Ds-bit and address fields

To DS bit value	From DS bit value	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Key: BSSID = basic service set identifier; DA = destination address; DS = destination stations; RA = receiver address; SA = source address; TA = transmitter address.

The *WEP* bit (when set to value '1') indicates that the *wired equivalent privacy* protocol is in use.

IEEE 802.11 Physical layer

The IEEE 802.11 standard provides three alternative physical medium implementations: two physical layer specifications for radio (operating in the 2 400-2 483.5 MHz band depending on local government regulations) and one for infrared interface (see Figure A6.1).

Frequency hopping spread spectrum radio PHYsical layer (FH-PHY)

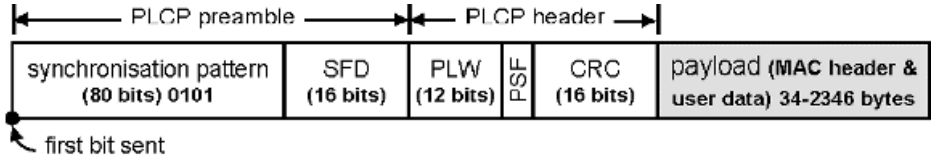
The *frequency hopping spread spectrum radio physical layer (FH-PHY)* of IEEE 802.11 provides for either 1 Mbit/s, or (optionally) for 2 Mbit/s operation. The 1 Mbit/s version uses 2-level *Gaussian frequency shift keying (GFSK)* modulation and the 2 Mbit/s version uses 4-level GFSK. The exact number and frequency of radio channels (i.e the precise physical medium) which should be used depend upon local government radio regulations and related radio technical standards. These are listed in Table A6.3.

Figure A6.4 illustrates the *physical layer convergence protocol (PLCP)* frame format used by IEEE 802.11 FH-PHY.

The *preamble* part of the frame (which comes at the start of each frame sent) is used to *synchronise* the radio transmission. During this period, radio receivers have to 'notice' that a signal is being sent, adjust their radio frequency circuitry to the exact frequency of the signal being sent by the transmitter and adjust their signal *automatic gain control (AGC)* to ensure that the signal is amplified appropriately. (Each received signal will have a different strength,

Table A6.3 Radio operations and technical standards relevant to IEEE 802.11

Region	Radio standard	Radio frequency band of operation	Number of hopping channels	Transmitter power restriction
United States	CFR 47 parts:	2400–2483.5 MHz	75–79	1 Watt max transmit power
	15.247			4 Watt max EIRP
	15.205			
	15.209			
Europe	ETS 300 328	2400–2483.5 MHz	20–79	100 mWatt max EIRP
	ETS 300 339			
Japan	RCR STD-33A	2471–2497 MHz	10–23	



Legend
CRC = cyclic redundancy check
MAC = medium access control
PLCP = physical layer convergence protocol
PLW = payload length word
PSF = PLCP signalling field
SFD = start of frame delimiter (always hex value 0CBD)

Figure A6.4 IEEE 802.11 frequency hopping spread spectrum radio physical layer (FH-PHY): PLCP (physical layer convergence protocol) frame format.

depending upon how far away the remote transmitter is — but there is an optimum signal level which should be sent to the *detector* circuitry.)

The *start of frame delimiter (SFD)* for FH-PHY is always set at the hexadecimal value '0CBD'.

A process called *CCA (clear channel assessment)* (one of the functions of the PLCP signalling field) performs the function of *collision detection* on behalf of the MAC layer. CCA initiates frame reception and forces back-off of transmission if the radio channel turn out to be busy.

Since radio transmission is very prone to errors (and in particular to *burst errors*[1]), data is *scrambled*[2] to reduce the problems of errors caused by interference.

A 16-bit *cyclic redundancy check (CRC)* code[3] is used as a header error check code for the *PLCP (physical layer convergence protocol)* header (i.e. the fields PLW and PSF).

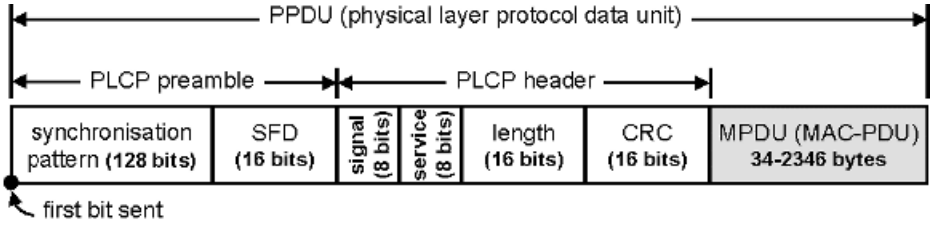
Direct sequence spread spectrum radio PHYsical layer (DS-PHY)

Like the frequency hopping spread spectrum radio physical layer (FH-PHY), the *direct sequence (DS) spread spectrum (DSSS) physical layer (DS-PHY)* of IEEE 802.11 provides for either 1 Mbit/s, or (optionally) for 2 Mbit/s operation in the 2.4 GHz (2400 MHz) *ISM (industrial scientific medical)* radio band. But unlike FH-PHY, the 1 Mbit/s version of the DS-PHY uses *differential binary phase shift keying (DBPSK)* modulation and the 2 Mbit/s version uses *differential quadrature phase shift keying (DQPSK).*

The radio *multiple access* scheme used in DS-PHY is CDMA (code division multiple access) — employing an 11 MHz chip rate and an 11-chip Barker sequence.

The physical layer convergence protocol (PLCP) and physical layer data unit frame format of DS-PHY are illustrated in Figure A6.5.

[1] See Chapter 8.
[2] Although *scrambling* in common parlance is synonymous with *encryption*, this is not its main purpose — and *scrambling* should not be taken to provide a suitable alternative to *encryption.*
[3] See Chapter 3.



Legend
CRC = cyclic redundancy check
MAC = medium access control
PLCP = physical layer convergence protocol
PLW = payload length word
PSF = PLCP signalling field
SFD = start of frame delimiter (always hex value F3A0)

Figure A6.5 IEEE 802.11 direct sequence spread spectrum radio physical layer (DS-PHY): PLCP (physical layer convergence protocol) frame format.

As with FH-PHY, the synchronisation preamble sequence of DS-PHY provides for a period during which the radio receiver can undertake signal *energy detection* (within 15 microsecs), antenna selection, frequency adjustment and signal gain settings.

The various frames have the following meanings and codings:

- the *start of frame delimiter (SFD)* for DS-PHY is always set at the hexadecimal value 'F3A0';
- the *signal* field indicates whether 1 Mbit/s DBPSK (signal = hexadecimal value '0A') or 2 Mbit/s DQPSK (signal = hexadecimal value '14') is in use;
- the *service* field (when set to hexadecimal value '00') indicates that the implementation is IEEE 802.11;
- the *length* field indicates the length of the MPDU (MAC protocol data unit) in number of bytes or octets;
- the PLCP header check provides for detection of bit errors in the signal, service and length fields. A 16-bit cyclic redundancy check (*CRC-16*) code is used and coded according to ITU-T (see Chapter 3).

Infrared PHYsical layer (IR-PHY)

The infrared PHY (IR-PHY) of IEEE 802.11 also provides for 1 Mbit/s transmission, with an option for 2 Mbit/s transmission. The 1 Mbit/s version employs *pulse position modulation* with 16 positions (*16-PPM*) and the 2 Mbit/s version uses *4-PPM (4-position pulse position modulation).*