1.3 IEEE 802.11

The IEEE standard 802.11 (IEEE, 1999) is the most famous family of WLANs in which many products are available. As the standard‘s number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring. The standard specifies the physical and medium access layer adapted to the special requirements of wirelessLANs.

The primary goal of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. Additional features of the WLAN should include the support of power management to save battery power, the handling of hidden nodes, and the ability to operate worldwide. The 2.4 GHz ISM band, which is available in most countries around the world, was chosen for the original standard. Data rates envisaged for the standard were 1 Mbit/s mandatory and 2 Mbit/s optional.

1.3.1 System architecture

Wireless networks can exhibit two different basic system architectures as : infrastructure- based or ad-hoc. Several nodes, called stations (STAi), are connected to access points (AP). Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP. The stations and the AP which are within the same radio coverage form a basic service set (BSSi).

The example shows two BSSs – BSS1 and BSS2 – which are connected via a distribution system. A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area. This network is now called an extended service set (ESS) and has its own identifier, the ESSID. The ESSID is the ‗name‘ of a network and is used to separate different networks.

Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN. The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs.

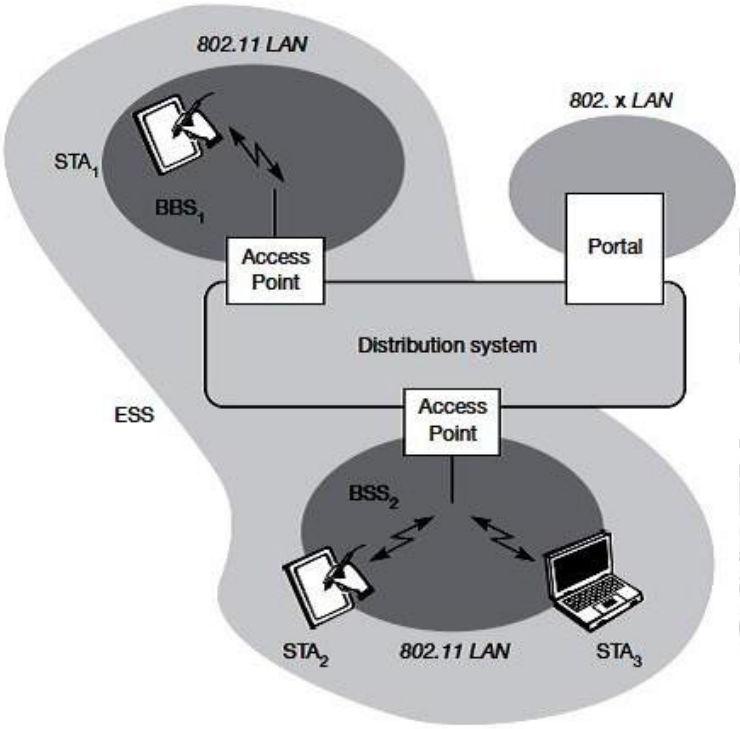


Fig. 1.3 Architecture of Infrastructure IEEE 802.11

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The architecture of the distribution system consists of bridged IEEE LANs, wireless links, or any other networks. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs. APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service. In addition IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS). In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2. This means for example that STA3 can communicate directly with STA2 but not with STA5. Several IBSSs can either be formed via the distance between the IBSSs or by using different carrier frequencies (then the IBSSs could overlap physically). IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topologyinformation as, e.g., HIPERLAN 1 or Bluetooth.

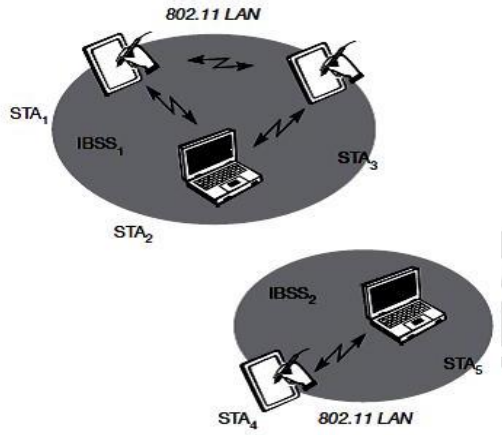


Fig. 1.4 Architecture of Adhoc IEEE 802.11

[Source: Text book - Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.2 Protocol architecture

IEEE 802.11 fits into the other 802.x standards for wired LANs. In the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet viaa bridge. The WLAN behaves like a slow wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes. The upper part of the data link control layer, the logical link control(LLC), covers the differences of the medium access control layers needed for the different media.

The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do. The physical layer is subdivided into the physical layer convergence protocol (PLCP) and the physical medium dependent sublayer PMD. The basic tasks of the MAClayer comprise medium access, fragmentation of user data,and encryption. The PLCP sublayer provides a carrier sense signal, called clear channel assessment(CCA), and provides a common PHY service access point (SAP) independent of the transmission technology. Finally, the PMD sublayer handles modulation and encoding/decoding of signals.

Apart from the protocol sublayers, the standard specifies management layers and the station management. The MAC management supports the association and re-association of a station to an access point and roaming between different access points. It also controls authentication mechanisms, encryption, synchronization of a station with regard to an access point, and power management to save battery power. MAC management also maintains the MAC management information base (MIB).

The main tasks of the PHY management include channel tuning and PHYMIB maintenance. Finally, station management interacts with both management layers and is responsible for additional higher layer functions (e.g., control of bridging and interaction with the distribution system in the case of an access point).

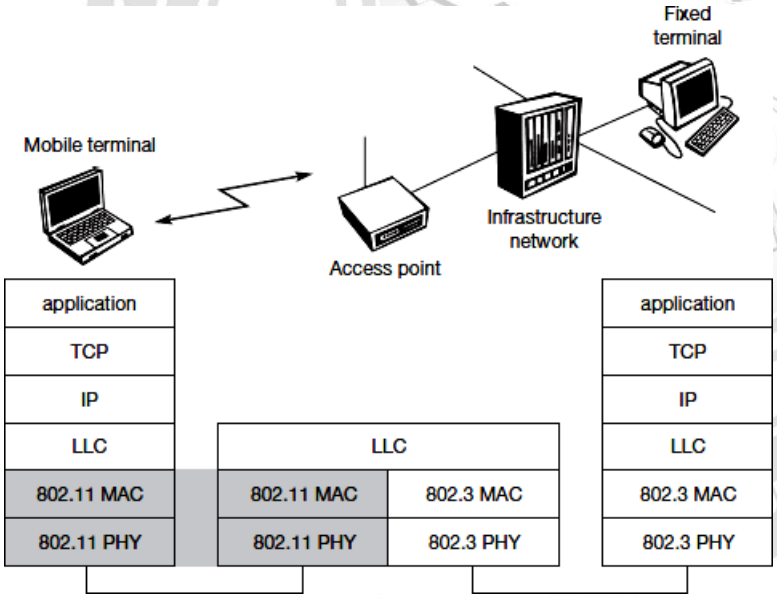
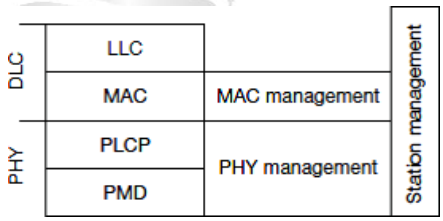


Fig. 1.5 IEEE 802.11 Protocol architecture and bridging

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]



[Source: Text book - Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.3 Physical layer

IEEE 802.11 supports three different physical layers: one layer based on infrared and two layers based on radio transmission (primarily in the ISM band at 2.4GHz, which is available worldwide). All PHY variants include the provision of the clear channel assessment signal (CCA). This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle.

The transmission technology determines exactly how this signal is obtained.

The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer (basic version of the standard).

1.3.4 Frequency hopping spread spectrum

Frequency hopping spread spectrum (FHSS) is a spread spectrum technique which allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences. The original standard defines 79 hopping channels for North America and Europe, and 23 hopping channels for Japan (each with a bandwidth of1 MHz in the 2.4 GHz ISM band). The selection of a particular channel is achieved by using a pseudo-random hopping pattern.

The standard specifies Gaussian shaped FSK (frequency shift keying), GFSK, as modulation for the FHSS PHY. For 1 Mbit/s a 2 level GFSK is used (i.e., 1 bit is mappedto one frequency), a 4 level GFSK for 2 Mbit/s (i.e., 2 bits are mapped to one frequency). While sending and receiving at 1 Mbit/s is mandatory for all devices, operation at 2 Mbit/s is optional. This facilitated the production of low-cost devices for the lower rate only and more powerful devices for both transmission rates in the early days of 802.11.

The physical layer used with FHSS has the frame that consists of two basic parts, the PLCP part (preamble and header) and the payload part. While the PLCP part is always transmitted at 1 Mbit/s, payload, i.e.MAC data, can use 1 or 2 Mbit/s.

The fields of the frame fulfill the following functions:

Synchronization: The PLCP preamble starts with 80 bit synchronization, which is a 010101... bit pattern. This pattern is used for synchronization of potential receivers and signal detection by the CCA.

Start frame delimiter (SFD): The following 16 bits indicate the start of the frame and provide frame synchronization. The SFD pattern is0000110010111101.

PLCP_PDU length word (PLW): This first field of the PLCP header indicates the length of the payload in bytes including the 32 bit CRC at the end of the payload. PLW can range between 0 and 4,095.

PLCP signaling field (PSF): This 4 bit field indicates the data rate of the payload following. All bits set to zero (0000) indicate the lowest data rate of 1 Mbit/s. The granularity is 500 kbit/s, thus 2 Mbit/s is indicated by 0010and the maximum is 8.5 Mbit/s(1111). This system obviously does not accommodate today‘s higher data rates.

Header error check (HEC): Finally, the PLCP header is protected by a16 bit checksum with the standard ITU-T generator polynomial
G(x) = x16 + x12 + x5 + 1.

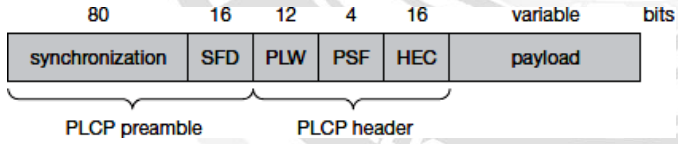


Fig. 1.6 Frame Format of IEEE 802.11 using FHSS

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.5 Direct sequence spread spectrum

Direct sequence spread spectrum (DSSS) is the alternative spread spectrum method separating by code and not by frequency. In the case of IEEE 802.11DSSS, spreading is achieved using the 11-chip Barker sequence (+1, –1, +1, +1, –1,+1, +1, +1, –1, –1, –1). The key characteristics of this method are its robustness against interference and its insensitivity to multipath propagation (time delay spread). However, the implementation is more complex compared to FHSS.IEEE 802.11 DSSS PHY also uses the 2.4 GHz ISM band and offers both 1 and2 Mbit/s data rates. The system uses differential binary

phase shift keying (DBPSK)for 1 Mbit/s transmission and differential quadrature phase shift keying (DQPSK)for 2 Mbit/s as modulation schemes. The symbol rate is1 MHz, resulting in a chipping rate of 11 MHz. All bits transmitted by the DSSSPHY are scrambled with the polynomial s(z) = z7 + z4 + 1 for DC blocking and whitening of the spectrum. Many oftoday‘s products offering 11 Mbit/s according to 802.11b are still backward compatible to these lower data rates.

The fields of the frame have the following functions:

Synchronization: The first 128 bits are not only used for synchronization, but also gain setting, energy detection (for the CCA), and frequency offset compensation. The synchronization field only consists of scrambled 1 bits.

Start frame delimiter (SFD): This 16 bit field is used for synchronization at the beginning of a frame and consists of the pattern 1111001110100000.

Signal: Originally, only two values have been defined for this field to indicate the data rateof the payload. The value 0x0A indicates 1 Mbit/s (and thus DBPSK), 0x14 indicates 2 Mbit/s (and thus DQPSK). Other values have been reserved for future use, i.e., higher bit rates.

Service: This field is reserved for future use; however, 0x00 indicates an IEEE 802.11 compliant frame.

Length: 16 bits are used in this case for length indication of the payload in microseconds.

Header error check (HEC): Signal, service, and length fields are protected by this checksum using the ITU-T CRC-16 standard polynomial.

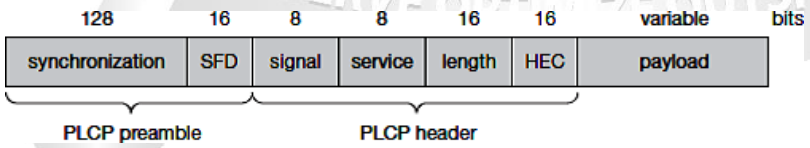


Fig. 1.7 Frame Format of IEEE 802.11 using DSSS

[Source: Text book - Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.6 Medium access control layer (MAC LAYER)

The MAC layer has to control medium access, but it can also offer support for roaming, authentication, and power conservation. The basic services provided by the MAC layer are the mandatory asynchronous data service and an optional time-bounded service. While802.11 only offer the asynchronous service in ad-hoc network mode, both service types can be offered using an infrastructure-based network together with the access point coordinating medium access. The asynchronous service supports broadcast and multi-cast packets, and packet exchange is based on a _best effort' model, i.e., no delay bounds can be given for transmission.

The following three basic access mechanisms have been defined for IEEE802.11:

- The mandatory basic method based on a version of CSMA/CA,
- An optional method avoiding the hidden terminal problem, and
- Finally a contention-free polling method for time-bounded service.

The first two methods are also summarized as distributed coordination function (DCF), the third method is called point coordination function (PCF). DCF only offers asynchronous service, while PCF offers both asynchronous and time-bounded service but needs an access point to control medium access and to avoid contention. The MAC mechanisms are also called distributed foundation wireless medium access control (DFWMAC).

For all access methods, several parameters for controlling the waiting time before medium access are important. The three different parameters that define the priorities of medium access. The values of the parameters depend on the PHY and are defined in relation to a slot time. Slot time is derived from the medium propagation delay, transmitter delay, and other PHY dependent parameters. Slot time is 50 μs for FHSS and 20 μs for DSSS. The medium, as shown, can be busy or idle (which is detected by the CCA).If the medium is busy this can be due to data frames or other control frames.

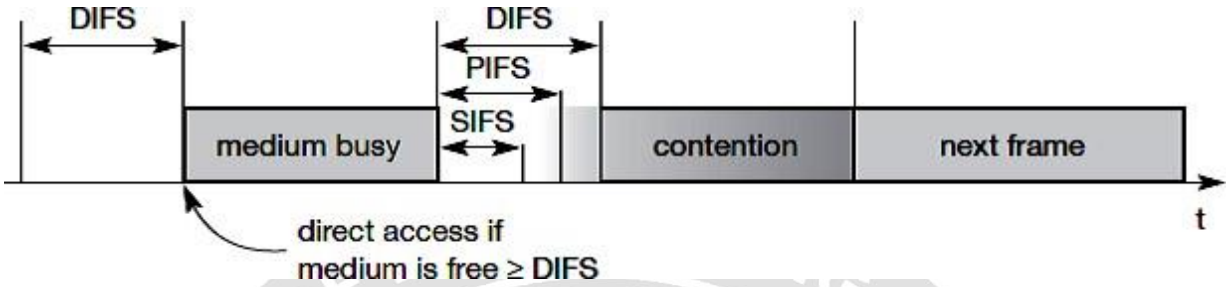


Fig. 1.8 Medium access and inter frame spacing

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

During a contention phase several nodes try to access the medium.

Short inter-frame spacing (SIFS): The shortest waiting time for medium access (so the highest priority) is defined for short control messages, such as acknowledgements of data packets or polling responses. For DSSS SIFS is10 μs and for FHSS it is 28 μs.

PCF inter-frame spacing (PIFS): A waiting time between DIFS and SIFS(and thus a medium priority) is used for a time-bounded service. An access point polling other nodes only has to wait PIFS for medium. PIFS is defined as SIFS plus one slot time.

DCF inter-frame spacing (DIFS): This parameter denotes the longest waiting time and has the lowest priority for medium access. This waiting time is used for asynchronous data service within a contention period. DIFS is defined as SIFS plus two slot times.

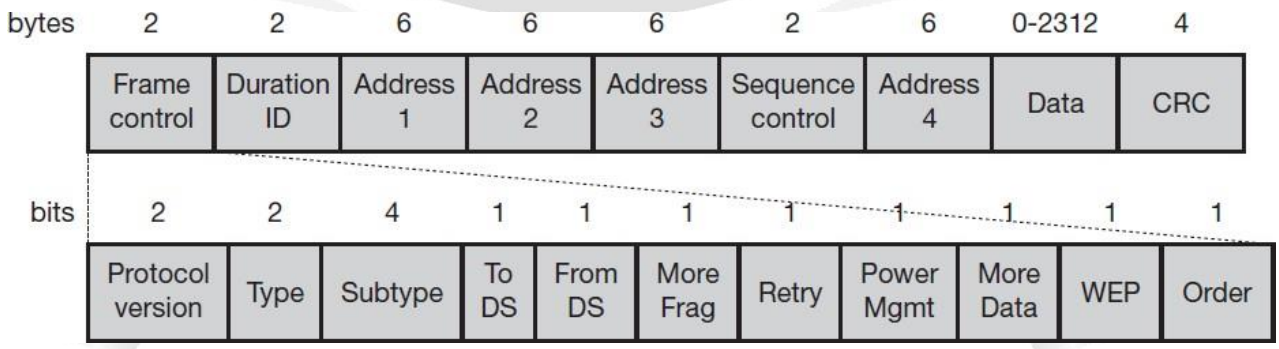


Fig. 1.9 Frame Control

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.7 MAC frames

The following figure shows the basic structure of an IEEE 802.11 MAC data ram together with the content of the frame control field.

● Frame control: The first 2 bytes serve several purposes. They contain several sub-fields.

● Duration/ID: If the field value is less than 32,768, the duration field contains the value indicating the period of time in which the medium is occupied (in μs). This field is used forsetting the NAV for the virtual reservation mechanism using RTS/CTS and during fragmentation. Certain values above 32,768 are reserved for identifiers.

● Address 1 to 4: The four address fields contain standard IEEE 802 MAC addresses (48 bit each), as they are known from other 802.x LANs. The meaning of each address dependson the DS bits in the frame control field.

● Sequence control: Due to the acknowledgement mechanism frames may be duplicated. Therefore a sequence number is used to filter duplicates.

● Data: The MAC frame may contain arbitrary data (max. 2,312 byte), which is transferredtransparently from a sender to the receiver(s).

● Checksum (CRC): Finally, a 32 bit checksum is used to protect the frame as it is common practice in all 802.x networks.

MAC frames can be transmitted

- Between mobile stations;
- Between mobile stations and
- An access point and between access points over a DS.

Two bits within the Frame Control field, _to DS‘ and _from DS‘, differentiate these cases and control the meaning of the four addresses used. The following Table will gives an overview of the four possible bit values of the DS bits and the associated inter predation of the four address fields.

to DS	from DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	–
0	1	DA	BSSID	SA	–
1	0	BSSID	SA	DA	–
1	1	RA	TA	DA	SA

Fig. 1.10 Interpretation of the MAC addresses in an 802.11 MAC frame

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Every station, access point filters on address 1. This address identifies the physical receiver(s) of the frame. Based on this address, a station can decide whether the frame is relevant or not. The second address, address 2, represents the physical transmitter of a frame. This information is important because this particular sender is also the recipient of the MAC layer acknowledgement. If a packet from a transmitter (address 2) is received by the receiver with address 1, this receiver in turn acknowledges the data packet using address 2 as receiver address as shown in the Figure. The remaining two addresses address 3and address 4, are mainly necessary for the logical assignment of frames (logical sender, BSS identifier, logical receiver). If address 4 is not needed the field is omitted.

For addressing, the following four scenarios are possible:

- **Ad-hoc network:** If both DS bits are zero, the MAC frame organizes a packet which is exchanged between two wireless nodes without a distribution system. DA indicates thedestination address, SA is the source address of the frame, which is identical to the physical receiver and sender addresses respectively. The third address identifies the basicservice set (BSSID, the fourth address is unused.
- **Infrastructure network, from AP:** If the bit only from DS is set, the frame physically originates from an access point. DA is the logical and physical receiver, the second

address identifies the BSS, and the third address specifies the logical sender, the source address of the MAC frame.

- **Infrastructure network, to AP:** If a station sends a packet to another station through the access point, only the _to DS' bit is set. Now the first address represents the physical receiver of the frame, the access point, via the BSS identifier. The second address is the logical and physical sender of the frame, while the third address indicates the logical receiver.

- **Infrastructure network, within DS:** For packets transmitted between two access points over the distribution system, both bits are set. The first receiver address (RA), represents the MAC address of the receiving access point. Similarly, the second address transmitter address (TA), identifies the sending access point within the distribution system. Now two more addresses are needed to identify the original destination DA of theframe and the original source of the frame SA.

1.3.8 MAC management

MAC management plays a vital role in an IEEE 802.11 station as it controls all the functions related to integration of a wireless station into a BSS, formation of an ESS, synchronization of stations etc.

- Synchronization: It is used to support finding a wireless LAN, synchronization of internal clocks, and generation of beacon signals.
- Power management: It is used to control transmitter activity for power conservation,e.g., periodic sleep, buffering, without missing a frame.
- Roaming: Functions for joining a network (association), changing access points, scanning for access points.
- Management information base (MIB): All parameters representing the current state of a wireless station and an access point are stored within a MIB for internal and external access. A MIB can be accessed via standardized protocols such as the simple network management protocol (SNMP).

1.3.9 Synchronization

An internal clock is maintained by each node of an 802.11 network. Timing synchronization function is specified by the IEEE 802.11 to synchronize the clocks of all nodes.

In power management synchronized clocks are needed, but also for coordination of the PCF and for synchronization of the hopping sequence in an FHSS system. The start of a super frame can be predicted by the local timer of the node. FHSS physical layers need thesame hopping sequences so that all nodes can communicate within a BSS.

A beacon contains a timestamp and other management information used for power management and roaming (e.g., identification of the BSS).The timestamp is used by a node to adjust its local clock. The node is not required to hear every beacon to stay synchronized; however, from time to time internal clocks should be adjusted. The transmission of a beacon frame is not always periodic because the beacon frame is also delayed if the medium is busy.

Within infrastructure-based networks, the access point performs synchronization by transmitting the (quasi)periodic beacon signal. However, the access point always tries to schedule transmissions according to the target beacon interval, i.e., beacon intervals are not shifted if one beacon is delayed. The timestamp of a beacon always reflects the real transmit time, not the scheduled time.

Ad-hoc networks, does not have an access point for beacon transmission. In this case, eachbeacon frame after the beacon interval. All other stations now adjust their internal clocks according to thereceived beacon and suppress their beacons for this cycle. If collision occurs, the beacon is lost.

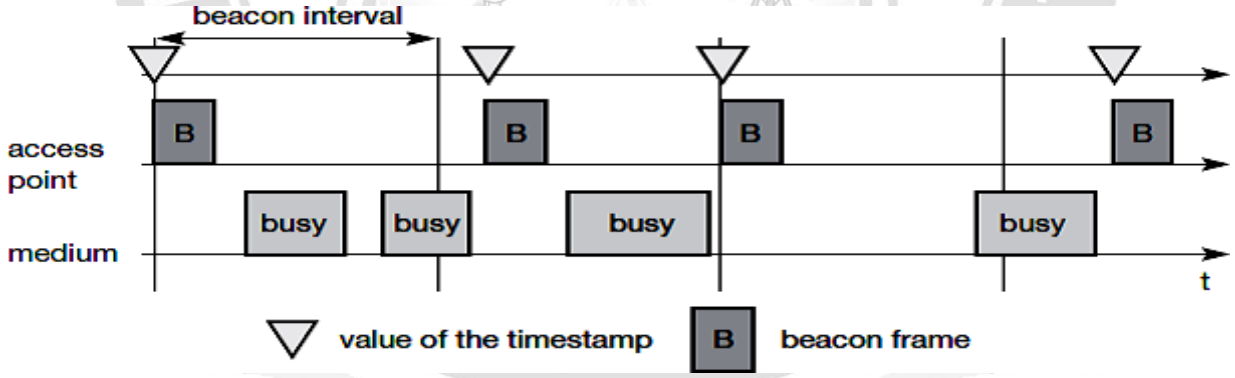


Fig. 1.11 Beacon transmission in a 802.11 network

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

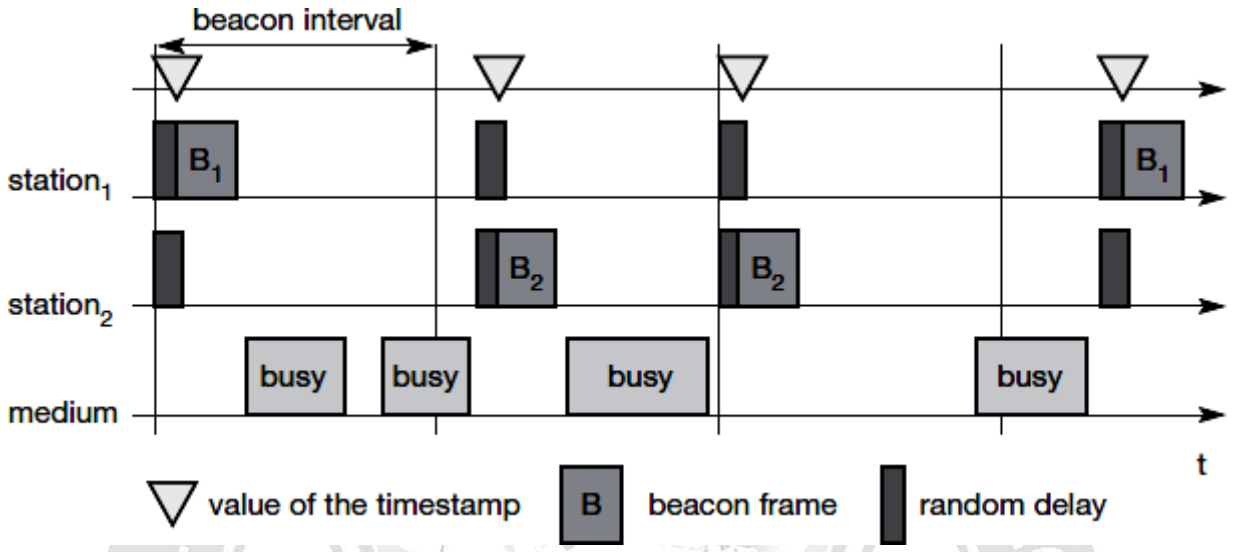


Fig. 1.11 Beacon transmission in a adhoc network

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.10 Power management

Wireless devices are battery powered. Hence power-saving mechanisms are critical for such devices. Standard LAN protocols are always ready to receive data, although receivers are idle most of the time in lightly loaded networks.

In IEEE 802.11 power management is to switch off the transceiver whenever it is not needed. This is simple for the sending device to achieve as the transfer is generated by the device itself. However, since the power management of a receiver cannot know in advance when the transceiver has to be active for a specific packet, it has to _wake up' the transceiver periodically.

Switching off the transceiver should be transparent to present protocols and able to support different applications. However, through put can be traded-off for battery life. Longer off-periods save battery life but average throughput will be reduce and vice versa.

The basic idea of power saving includes two states for a station: sleep and awake, and buffering of data in senders. If a sender aims to communicate with a power-saving station, if the station is a sleep it needs to buffer data. On the other hand the sleeping station has to wake up periodically and stay awake for a certain time. During this time, all senders can reveal the destinations of their buffered data frames. If a station detects that it is a destination of a buffered packet it has to stay awake until the transmission takes place. All stations have to wake up or be awake at the same time.

Compared to ad-hoc networks infrastructure-based networks has a simpler power

management. The access point buffers all frames of stations operating in power-save mode. With every beacon sent by the access point, a traffic indication map (TIM) is

transmitted. The TIM contains a list of stations for which unicast data frames are bufferedin the access point.

If the TIM indicates a unicast frame for the station, the station stays awake for transmission. Stations will always stay awake for multi-cast/broadcast transmission.

A sleeping station still has the TSF timer running.

The following figure shows an example with an access point and one station.

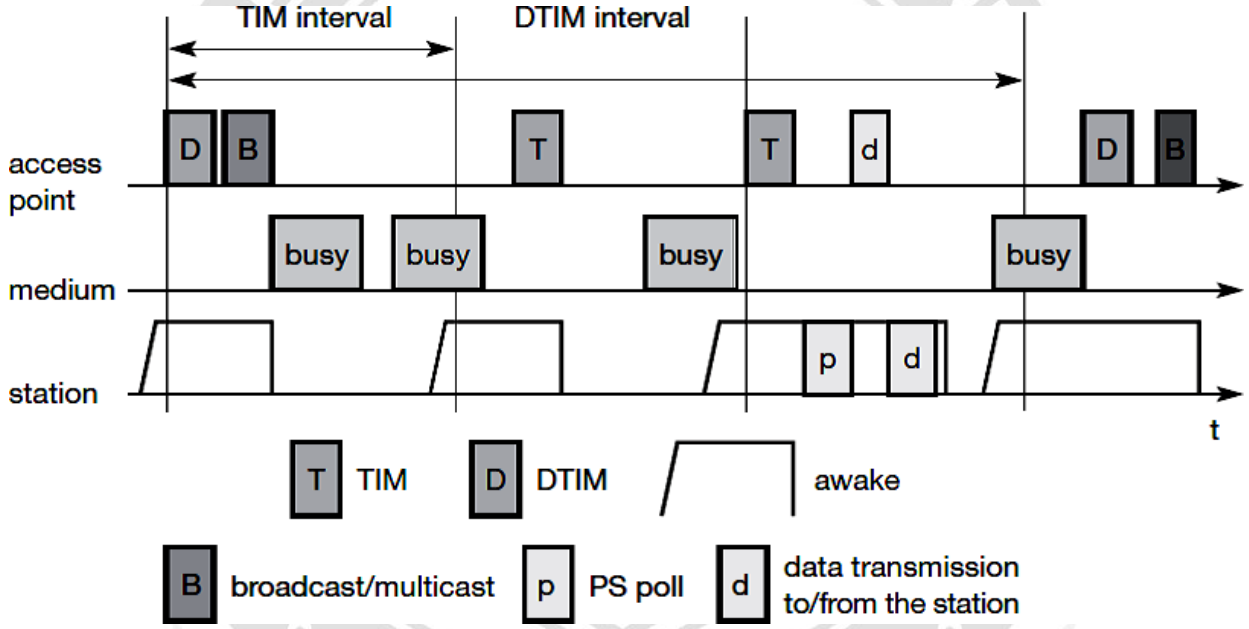


Fig. 1.12 Access Point with one station

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.11 Power management in IEEE 802.11 Network

The state of the medium is indicated. The access point transmits a beacon frame each beacon interval. This interval is now the same as the TIM interval. For sending broadcast/multicast frames, the access point maintains a delivery traffic indication map(DTIM) interval. The DTIM interval is always a multiple of the TIM interval.

In the first case, the access point has to transmit abroad cast frame and the station stays awake to receive it. After receiving the broadcast frame, the station returns to sleeping mode. Before the next TIM transmission starts, the station wakes up. This time the TIM isdelayed due to a busy medium so, the station stays awake. The access point has nothing to send and the station goes back to sleep.

At the next TIM interval, the station is the destination for a buffered frame indicated by theaccess point. The access point then transmits the data for the station; the station acknowledges the receipt and may also send some data and it is acknowledged by the access point, afterwards, the station switches to sleep mode again. Finally, the access point has more broadcast data to send during the next DTIM interval, which is again delayed bya busy medium. A station may stay awake if the sleeping period would be too short.

This mechanism clearly shows the trade-off between short delays in station access and saving battery power. The shorter the TIM interval, the shorter the delay, but the lower thepower-saving effect.

The power management for ad-hoc networks is much more complicated than in infrastructure networks. In this case, there is no access point to buffer data in one location but each station wants to buffer data if it wants to communicate with a power-saving station. Buffered frames list are announced by the stations during a period when they are all awake. Destinations are announced using ad-hoc traffic indication map (ATIMs) – the announcement period is called the ATIM window.

All stations stay awake for the ATIM interval as shown in the first two steps and go to sleep again if no frame is buffered for them. In the third step, station1 has data buffered forstation2. This is indicated in an ATIM transmitted by station1.

Station2 acknowledges this ATIM and stays awake for the transmission. After the ATIM window, station1can transmit the data frame, and station2 acknowledges its receipt. In thiscase, the stations stay awake for the next beacon. More ATIM transmissions take place, more collisions happen and more stations are delayed. The access delay of large networks isdifficult to predict. QoS guarantees cannot be given under heavy load.

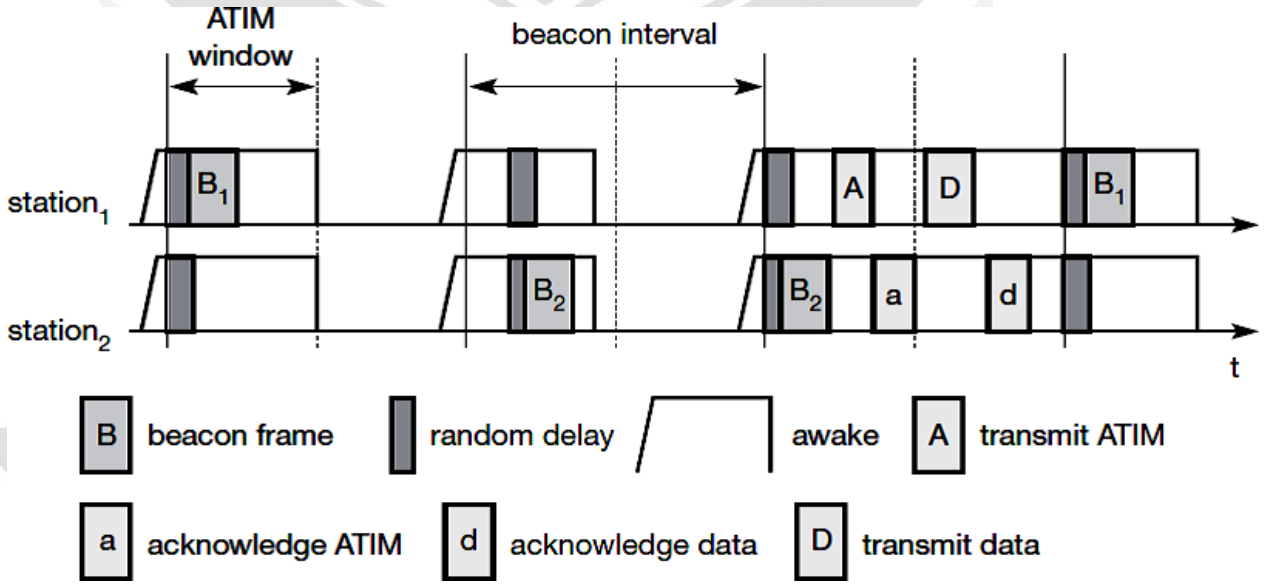


Fig. 1.13 Power management in IEEE 802.11 ad-hoc network

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.12 Roaming

Access point more than one is required to cover all rooms when the wireless networks are within the buildings. Depending on the structure of the walls, one access point has a transmission range of 10–20 m. Each story of a building needs its own access point(s) as quite often walls are thinner than floors. If a user walks around within a wireless station, the station has to change from one access point to another to provide uninterrupted service. Moving between access points is refers to roaming.

The steps for roaming between access points are:

- When the current link quality to its access point AP1 is too poor. The station then starts scanning for another access point.

- Scanning will search for another BSS and can also be used for setting up a new BSS in case of ad-hoc networks. IEEE 802.11 specifies scanning on single or multiple channels and differentiates between passive scanning and active scanning. Passive scanning means listening into the medium to find other networks, i.e.,receiving the beacon of another network issued by the synchronization function within an access point. Active scanning comprises sending a probe on each channel and waiting for a response. Beacon and probe responses contain the information necessary to join the new BSS.
- The station then selects the best access point for roaming based on, signal strength, andsends an association request to the selected access point AP2.
- The new access point AP2 answers with an association response. If the response is successful, the station has roamed to the new access point AP2.

The access point accepting an association request indicates the new station in its BSS to the distribution system (DS). The DS then updates its database, which contains the currentlocation of the wireless stations. This database is needed for forwarding frames between different BSSs, i.e. between the different access points controlling the BSSs, which combine to form an ESS.

The standard IEEE 802.11f should provide a compatible solution for all vendors. This alsoincludes load-balancing between access points and key generation for security algorithms based on IEEE 802.1x (IEEE, 2001).