Chapter 8

Appendix

8.1 IEEE 802.11 and WiFi

8.1.1 802.11 overview

In recent years, the demand for rendering multimedia applications over wireless has motivated the development and enhancement of IEEE 802.11 wireless local area network (LAN). Compared to the traditional Ethernet LAN, Wireless LAN has the merits of easy installation, low cost and supporting certain degree of mobility. 802.11 is a part of the 802 standard family for local area networks. This family defines the physical and data link layer specified in the International Organization for Standization (ISO) Open Systems Interconnection (OSI) basic reference model. More specifically, 802.11 defines the medium access control (MAC) layer and physical (PHY) layer. Its relation with other IEEE 802 standards is illustrated in Figure 8.1.

The illustrated standards in Figure 8.1 are described as follows:

- 802– Overview and Architecture. This standard is an overview of the

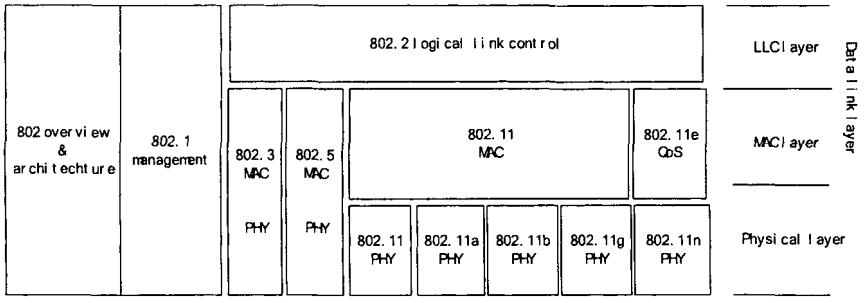

Figure 8.1: IEEE 802 standard family for local area networks

IEEE 802 standard family.

- 802.1B/1E/1F– LAN and MAN Management/ System Load Protocols/ Common Definitions and Procedures. This set of standards define LAN/ MAN management related services, protocols, architectures and procedures.
- 802.2– Logical Link Control. This standard defines the Logic link control sublayer specification.
- 802.3– CSMA/CD Access Method and Physical Layer Specifications. This standard defines the Ethernet MAC layer and PHY layer specifications.
- 802.5– Token Ring Access Method and Physical Layer Specifications. This standard defines the MAC layer and PHY layer for Token Ring Networks.
- 802.11– Wireless LAN MAC and PHY Specifications. This is the first 802.11 standard which defines the CSMA/CA MAC scheme and three PHY schemes: Infrared, frequency hopping spread spectrum and direct sequence spread spectrum.
- 802.11a – Wireless LAN MAC and PHY Specifications: High Speed PHY Layer in the 5 GHz Band. This standard defines the OFDM PHY specification operating at "Unlicensed national information infrastructure" (U-NII) 5 GHz frequency band.
- 802.11b – Wireless LAN MAC and PHY Specifications: High-Speed PHY Layer Extension in the 2.4 GHz Band. This standard is an enhancement of the 802.11 PHY layer in the 2.4 GHz band. It is backward compatible with 802.11.
- 802.11g – Wireless LAN MAC and PHY Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band. This standard is a further enhancement of 802.11 and 802.11b. It is backward compatible with 802.11 and 802.11b.
- 802.11e – This standard has not been finalized yet and is handled by 802.11 Task Group (TG) e. The TG e is working on the enhancement of 802.11 MAC layer to provide better quality of service in 802.11 network. The finalized standard shall be named as 802.11e.
- 802.11n – This standard has not been finalized yet. It is currently handled by 802.11 Task Group n. The TG n is responsible for the physical layer technologies for future wireless LAN supporting minimum 100 Mbps MAC data rate. The finalized standard shall be named as 802.11n.

The last letter in the standard name indicates the Task Group that is responsible for improving certain aspects of the standard. For instance, 802.11 task group A is working on wireless LAN standard in the 5 GHz band. The standard approved by Task Group A is named as 802.11a.

Referring to Figure 8.1, 802.11 standard family (802.11 and its enhancements 802.11a/b/g/n) is a set of MAC and PHY specifications that work with the LLC encapsulation defined in 802.2. In fact, the main difference of these standards is their physical layer technologies; their MAC layer scheme remains unchanged.

The first version of 802.11 was approved in 1997. It adopts three types of PHY options: frequency hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS) and Infrared (IR) techniques, though the last one is not widely deployed. By then, the maximum data rate is 2 Mbps. 802.11 was initially designed in the 2.4 GHz unlicensed "industrial, scientific and medical" (ISM) band. This band of frequencies is also crowded with microwave and several other systems. People then began to seek other frequency band options. In 1999, the second version, 802.11a, was approved, and it is operating in "unlicensed national information infrastructure" (U-NII) 5 GHz band. 802.11a adopts OFDM as its physical layer technology. The new technology of 802.11a PHY boosts the data rate from 2 Mbps to 54M bps. 802.11b was also approved in 1999, and it is still operating in the 2.4GHz band. The 802.11b PHY enhances the 802.11 DSSS PHY scheme with HR-DSSS PHY scheme using advanced coding and modulations, thus the data rate is increased from 2 Mbps to 11 Mbps. Besides, 802.11b is backward compatible with 802.11. The data rate gap between 802.11a and 802.11b motivates further enhancements on PHY schemes in the 2.4 GHz band. In 2003, 802.11g was approved, which is backward compatible with both 802.11 and 802.11b. 802.11g still operates in the 2.4 GHz ISM band, and it also adopts OFDM into the PHY layer. The maximum data rate of 802.11g is also 54 Mbps. Currently, Task Group n is working on the advanced PHY techniques for future wireless LAN. It aims to support data rate up to 100 Mbps excluding MAC overhead. Many state-of-the-art technologies in communications, e.g.,MIMO, space-time signal processing, LDPC coding, are very likely to be finalized in the published standard. Future wireless LAN also requires QoS be provided for the diverse multimedia applications. This motivates Task Group e to develop QoS mechanisms over wireless LAN. The schemes being discussed include admission control, various contention window sizes for different applications, arbitration interframe space, etc. Table 8.1 summarizes the key parameters of each 802.11 version.

Recently, the Wireless Ethernet Compatibility Alliance (WECA) has proposed their certification program for 802.11 products. Any product passed their interoperable test program can be named as WiFi (wireless fidelity) products. As a consequence, 802.11 is sometimes referred to as WiFi.

8.1.2 802.11 network architecture

802.11 defines three types of network architecture: Independent basic service set (IBSS), basic service set (BSS) and extended service set (ESS). The wireless terminal in the 802.11 network is termed "station".

Standard	Frequency Band (GHz)	Published Time	PHY Technologies	Maximum Rate (Mpbs)
802.11	2.4	1997	DSSS, FHSS and Infrared	2
802.11a	5	1999	OFDM	54
802.11b	2.4	1999	HR-DSSS	11
802.11g	2.4	2003	DSSS, OFDM	54
802.11n	Not yet	Not yet	OFDM, MIMO, LDPC, turbo,space-time codes	100 (excluding MAC overhead)

Table 8.1: Current 802.11 standards comparison

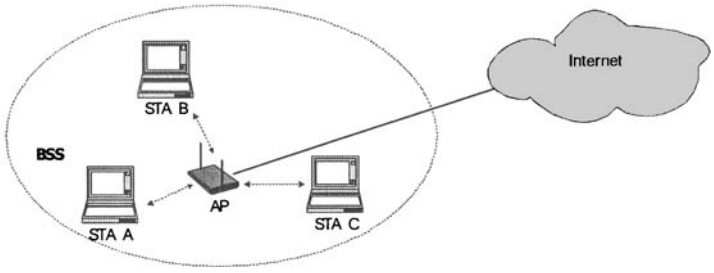

Figure 8.2: An example of Basic Sevice Set (BSS)

- BSS is also referred to as infrastructure network. In a BSS network, stations do not communicate with each other directly, but they communicate with a special terminal called access point (AP). The AP forwards the frames from the originating station to the destination station.

  Example 45 *An example of an infrastructure network is shown in Figure 8.2 where stations communicate with the AP directly. The AP is usually connected to the backbone wired network. Therefore, stations in the BSS network have access to the backbone network with the aid of the AP. Frames destined to the backbone network are distinguished by the AP and forwarded to the corresponding backbone routers.*

- IBSS is also referred to as Ad Hoc network. In an IBSS network, stations communicate with each other directly and there is no access point

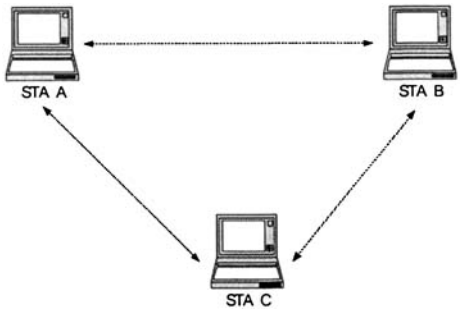

Figure 8.3: An example of Independent Basic Service Set (IBSS)

participating in the coordination. Therefore stations in the network are self-organized.

Example 46 *An IBSS network is shown in Figure 8.3 which contains three stations communicating directly with each other. Figure 8.3 can represent the scenario of a small conference meeting where stations share their information during the conference period.*

An IBSS network is usually within short range and contains a small number of devices. Besides, stations in IBSS cannot access the backbone network, as there is no AP forwarding their packets.

- An ESS is formed when several APs are connected. The component connecting the APs is called "distribution system" (DS). The DS is responsible for distributing the frames from the originating AP (i.e., the AP that communicates with the originating station) to the destination AP (i.e., the AP that communicates with the destination station). For frames directed to/from the backbone network, the DS is responsible for distributing these frames to the corresponding routers/APs.

  Example 47 *An example of an ESS network is shown in Figure 8.4. The illustrated ESS contains three BSSs and the corresponding APs are connected by a hub. The hub in this case plays the role of a DS.*

  Note that a DS is not necessarily of wired configuration. APs can also be connected through the wireless medium using the so called "wireless bridge" configurations.

From protocol stack point of view, the 802.11 family is similar to other 802 MAC and PHY specifications such as 802.3 and 802.5. However it faces

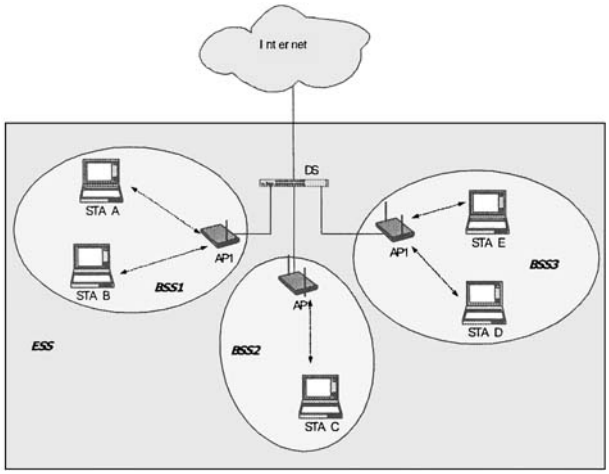

Figure 8.4: An example of Extended Service Set (ESS)

new challenges in the wireless medium. The path loss, shadowing and fading in the wireless environment give rise to high error rate in the communication link. Besides, unlike wired devices that can transmit and receive simultaneously, wireless devices are usually half duplex and cannot transmit and receive at the same time. These differences pose new challenges for the MAC and PHY layers in wireless LAN. In the following, we discuss the MAC and PHY technologies in 802.11 networks.

8.1.3 MAC layer technologies

Hidden node problem and collision avoidance

Generally speaking, 802.11 uses a contention based medium access scheme similar to Ethernet (802.3). However, the CSMA/CD scheme defined in 802.3 has its limitations when applied to the wireless environment. First of all, in Ethernet, the carrier sensing and collision detection are implemented by monitoring the wire's signal level by each station. A collision is assumed when the station detects an unusually high signal level (caused by simultaneous transmission of multiple stations). Secondly, the transmitted signal in Ethernet is assumed to reach all the stations connected on the wire. This is because the wired link has very low error rates and is regarded as very stable. However these two properties of Ethernet do not hold in wireless LAN. First of all, the path loss, shadowing and fading make the wireless signal level vary dramatically. Therefore, it is unlikely to justify whether the medium is busy or whether there is a collision by purely monitoring the received signal level. Secondly, because of the high error rate presented in the wireless link, the signal transmitted by one station is not guaranteed to be received correctly by another station. Furthermore, the

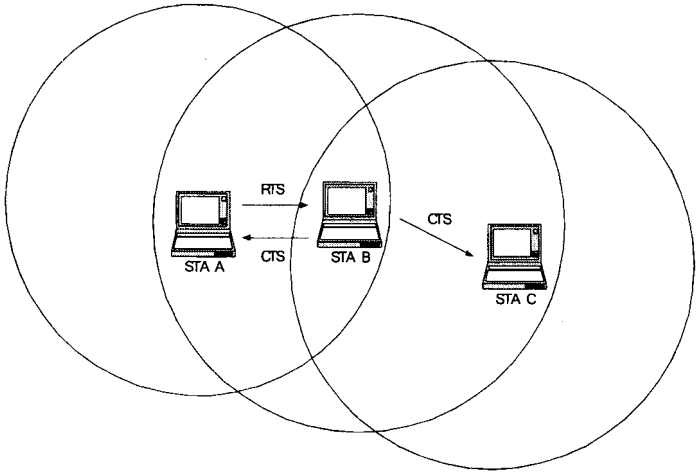

Figure 8.5: An example of the hidden node scenario

transmitted signal may not be even detected by another station, leading to the so-called "hidden node" scenario in wireless LAN.

Example 48 *Figure 8.5 shows an example of the "hidden node" scenario. There are three wireless devices– stations A, B and C. The circle centered at each station represents their transmission range. Stations outside of the circle cannot receive the signal sent by the station. In this example, A and B are within each other's range. B and C are within each other's range. However due to some reasons such as long distance, A and C cannot communicate with each other. In this scenario, when A is transmitting, C still regards the medium as free as it does not detect the signal transmitted from A. As a result, C may start transmitting while A has not finished, leading to collisions. Despite of the retransmission efforts, C will always interfere with A's transmission. In this case, C is regarded as a "hidden node" to A. Similarly, A is also a hidden node to C.*

To prevent collisions, 802.11 MAC layer uses a collision avoidance (CA) scheme. The transmitting station first sends a short message called "request to send" (RTS) when it has data to send. The receiver then responds with a short message called "clear to send" (CTS). These short messages contain information of how long the wireless medium needs to be reserved for their communications. All the stations hearing either of the two messages should set the medium state as busy and hold their transmission during this period. Therefore, the hidden nodes are silenced by the RTS and/or CTS. In the example in Figure 8.5, although the RTS message sent from A does not reach C, the CTS message sent from B is received by C. Therefore station C shall hold its transmission until A and B finish their communications. Note that in order to save the signaling overhead, 802.11 also has an option of sending data frames

without exchanging RTS/CTS if the data frame is shorter than a threshold. This threshold is pre-set by the 802.11 network administrator.

In addition to the RTS and CTS exchange, data frames also indicate the medium reservation period. Moreover, acknowledgment frames are sent from the receiver to the sender when data frames are received correctly. These acknowledgment frames also indicate the amount of time that the medium will be reserved for the rest of the communication. As a result, the RTS/CTS signaling together with the data/acknowledgment medium reservation scheme prevent the hidden node problem in 802.11 networks.

Carrier sensing scheme

As mentioned earlier, the carrier sensing scheme used in Ethernet cannot apply to the wireless network due to the dramatic signal level variations. Instead, the carrier sensing in 802.11 is realized by physical layer's carrier sensing/clear channel assessment (CA/CCA) procedure together with the "network allocation vector" (NAV) in the MAC layer. In the physical layer, the carrier sensing is realized by a CA/CCA procedure using schemes such as signal detection and energy detection. While in the MAC layer, the carrier sensing is realized by monitoring NAV. NAV is a value stored in the MAC layer in each station. It indicates how much time the medium will still be busy. This value is updated by each station when it detects a larger NAV value in the received frame even if the frame is not addressed to this station. The NAV value counts down with time. When NAV reaches zero, the wireless medium is deemed as free from the MAC layer perspective. Otherwise, the station should hold its transmission until NAV goes down to 0. For example, when a station sends a RTS to the medium, it shall calculate the amount of time that is needed to transmit the responding CTS and the following data frames plus the pre-determined interframe periods. The station then sets this time in the frame header when the RTS frame is transmitted. All the stations receiving the RTS shall update their NAV values and count down with time.

Interframe spacing

By the time the station's NAV reaches zero and the PHY also reports an idle medium, the station must wait for an interframe space (IFS) before it starts the backoff timer to contend for the medium, which is shown in Figure 8.6. IFS plays an important role in regulating medium access. The type of frame that is to be sent determines the IFS that the station must wait in addition to the backoff timer. It is obvious that frames with shorter IFS have higher priority gaining the medium than frames with longer IFS. 802.11 defines four types of IFS for different frame types. In the following, we describe the four types of IFS in ascending order.

- Short interframe space (SIFS)

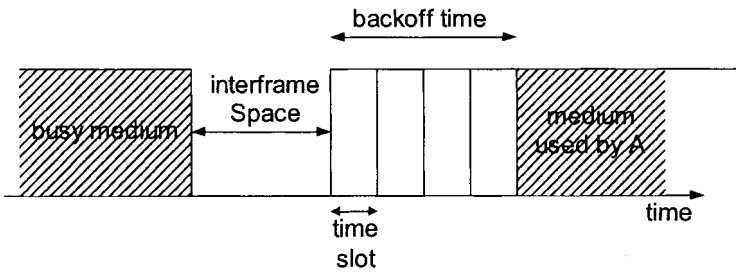

Figure 8.6: Interframe space and contention window

SIFS is the shortest IFS defined in 802.11. It is applied to the frames with the highest priority. For instance, when a station receives RTS, CTS is transmitted after SIFS period of time in order to respond to the originating station as soon as possible. Acknowledgments of correctly received frames also use SIFS to feed back the information to the sender quickly. When a data block exceeds the maximum frame length, fragmentation is required. The fragmented frames belonging to the same block use SIFS to facilitate fast assembly of the original data block without interruption from other stations. These frames have the highest priority and are transmitted after SIFS amount of time once the medium becomes idle, preempting over other types of frames.

- PCF interframe space (PIFS)

PIFS is used in contention free operation mode. In addition to contention based access method, 802.11 also defines a contention free operation mode. Contention free operation is regulated by a point coordination function (PCF). During contention free period, the AP polls each station and allows stations to transmit alternatively. The frames transmitted during contention free period use PIFS. It is shorter than the interframe space operated in contention-based period. Therefore, frames transmitted in contention free mode have higher priority gaining the medium than the regular contention-based frames.

- DCF inter-frame space (DIFS)

DIFS is the most commonly used IFS in 802.11 networks. The CSMA/CA and random backoff schemes are regulated by the distributed coordination function (DCF) in the MAC layer and DIFS is the default IFS coordinated by DCF.

- Extended inter-frame space (EIFS)

EIFS is used by the DCF whenever a frame is not received correctly with a valid CRC. When such a frame is determined to be erroneous, the next transmission attempt shall use EIFS instead of DIFS. Once the station receives a correct frame with a valid CRC, the following frames shall start using the regular DIFS.

EFIS is designed to provide enough time for another station to acknowledge, to this station, an incorrectly received frame before this station commence transmission. Reception of an error-free frame re-synchronizes the station with the actual medium idle/busy state; thus, EIFS is terminated, and the DIFS is used instead.

Random backoff contention scheme

After the medium has been sensed as idle for the corresponding interframe space period, the station shall contend for the wireless medium through DCF, if it has data to send.

Basically DCF regulates the CSMA/CA and random backoff contention procedure. The station randomly selects a value between 0 and its current contention window ($CW_{current}$). This value corresponds to the number of time slots the station must wait before it may transmit. For example, if station A has a contention window $CW_{current} = 15$, and it randomly selects a value between 0 and 15, e.g., 4, then the station must wait for additional 4 time slots before it may transmit. During this period, the station keeps sensing the medium. If the medium is sensed as free during these time slots, then A starts transmission as shown in Figure 8.6. However, if station B selects a shorter backoff value, e.g., 2 time slots, and starts transmission before A, then A should hold its data and update its NAV value after it receives frames from the medium. Once B completes its transmission, A resumes its count down procedure and starts transmission when the remaining 2 time slots elapse, which is shown in Figure 8.7.

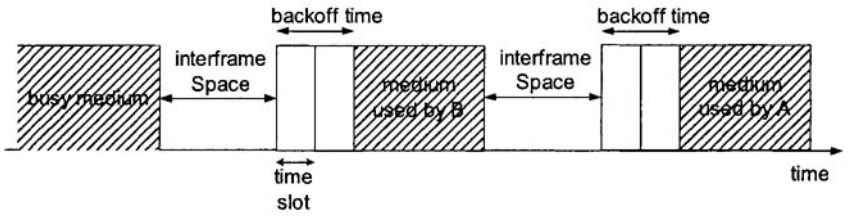

Figure 8.7: Random backoff and medium contention of two users

$CW_{current}$ is of the following form:

$$CW_{current} = 2^n - 1,$$

where n is an integer. The value of n is restricted by the inequality

$$CW_{\min} \leq CW_{current} \leq CW_{\max},$$

where $CW_{\min}$ and $CW_{\max}$ are pre-set values. For example, if $CW_{\min} = 15$ and $CW_{\max} = 127$. Then n can only take values from 4 to 7. Initially, $CW_{current}$ is

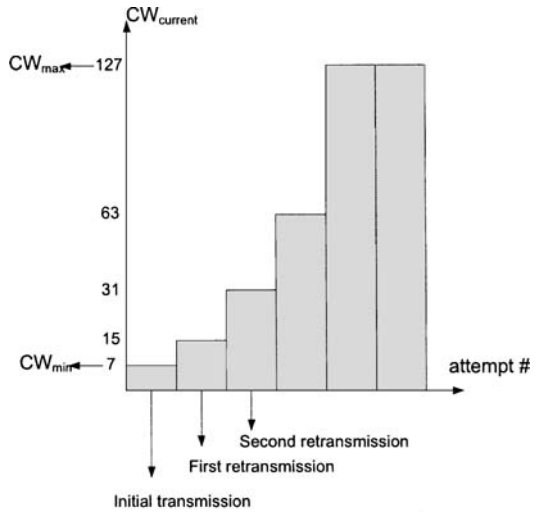

Figure 8.8: Exponential increase of CW

set to $\mathrm{CW}_{\min}$. $CW_{current}$ is also reset to $CW_{\min}$ when a frame is transmitted successfully. Every time the transmitted frame does not receive a corresponding acknowledgment or the responding message within a defined time, n increases by 1, i.e., $CW_{current}$ almost doubles as shown in Figure 8.8, until it reaches the allowed maximum value. In the following transmissions, the station shall use the new $CW_{current}$ value. In the meantime a retry count is increased by 1. The retry count also has an allowable maximum value. An error is reported to the upper layers when the maximum retry count is reached, and the frame is discarded.

Framing format

The information delivered from the MAC layer of one station to the peer layer of another station is encapsulated into a defined format. All MAC frames are generated following the format shown in Figure 8.9. All frames are made up of three parts: a frame header, a frame body and a frame check sequence (FCS). The subfields are described as follows:

- Frame Control field is comprised of the following subfields as shown Figure 8.10: Protocol Version, Type, Subtype, To DS, From DS, More Fragments (More Frag), Retry, Power Management (Power Mgmt), More Data, Wired Equivalent Privacy (WEP) and Order.

  - Protocol Version is a 2-bit field indicating which version of 802.11 MAC is functioning. At present, only one 802.11 MAC has been

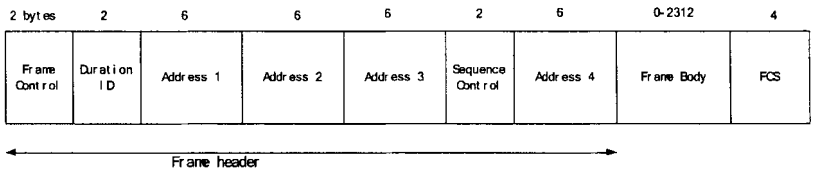

Figure 8.9: 802.11 MAC frame format

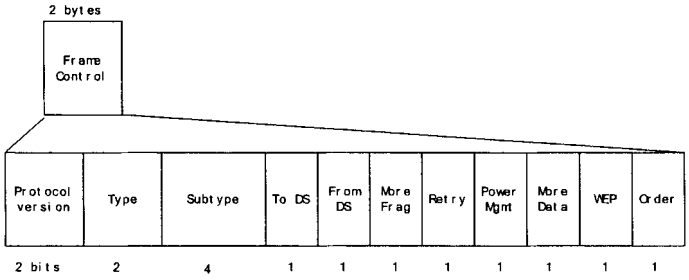

Figure 8.10: Frame control field

published, so this value shall be set to 0 and all other values are reserved.

- Type and Subtype fields together define the unique identity of the frame. There are three types of frames defined in the standard:

  Control frames, which are used to gain access of the wireless medium.

  Management frames, which are used to exchange management information. These frames are transmitted as data frames, but not passed to the upper layer.

  Data frames are used for data transmission. These frames are passed to upper layers.

  For each frame type, the subtype field further specifies the exact function of the frame. The valid type and subtype combination is shown in Table. 8.2. Other combinations are reserved.

- To DS/From DS field indicates whether the frame is directed to/coming from DS.
- More Fragments field indicates whether this frame is a fragment of a large MAC SDU.
- Retry field indicates whether the frame is a retransmission frame.
- Power Management field indicates whether the station is in power save mode.

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
01	Control	1010	Power save (PS)-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	Ack
01	Control	1110	Contention free (CF)-End
01	Control	1111	CF-End+CF-Ack
10	Data	0000	Data
10	Data	0001	Data+CF-Ack
10	Data	0010	Data+CF-Poll
10	Data	0011	Data+CF-Ack+CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack+CF-Poll (no data)

Table 8.2: Frame Type and Subtype combinations

  - More Data field indicates whether there is more data to send to/from the station.
  - WEP field indicates whether the Wired Equivalent Privacy (WEP) encryption method is used in the frame body.
  - Order field indicates whether the station is reordering the MAC SDUs. The reordering is to adjust the delivery order of broadcast/multicast MAC SDUs relative to unicast SDUs. This service is designed to improve the likelihood of successful delivery.

- Duration ID, in most cases, is set to be the amount of time that the medium is reserved for the station. In certain frame types, this field contains the station's Association ID.

- Address 1, 2, 3 and 4 fields represent BSS Identification, source address, destination address, transmitting station address, and receiving station

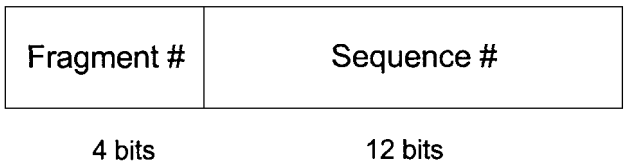

Figure 8.11: Sequence control field

address, respectively. Certain frame types may not contain some of the address fields.

- Sequence Control field is comprised of two parts as shown in Figure 8.11
- The Sequence Number field is a 12-bit field indicating the sequence number of an MSDU or MAC management PDU (MMPDU). If the MSDU or MMPDU is larger than the maximum frame length, it shall be fragmented into small segments to fit into the frame format. The Fragment Number then indicates the fragment number belonging to the current MSDU or MMPDU.
- Frame Body field is a variable length field and contains information directed to the peer MAC layer. The detailed information is dependent on the specific frame type and subtype.
- FCS is a 32-bit CRC calculated over all the fields in the MAC header and the Frame Body.

Example 49 *An example of MAC frame exchanges between a station and an AP is shown in Figure 8.12. The message exchange in this example is described as follows:*

1. *After the station powers up, a Probe Request is first transmitted to detect available APs around it. Probe Request contains the station's capability information such as supportable rate.*
2. *If the Probe Request is received successfully by an AP, the AP shall respond with a Probe Response to inform the AP's information such as timing, beacon signal, supportable rate and PHY layer parameters.*
3. *If the station decides to connect to the AP, an Authentication procedure is invoked to determine the validity of the station on this network. This is a two-way Authentication procedure.*
4. *After the station passes the authentication procedure, it sends an Association Request to associate itself to the current AP. Association Request contains the stations's information such as power save mode parameters as well as supportable rate information.*

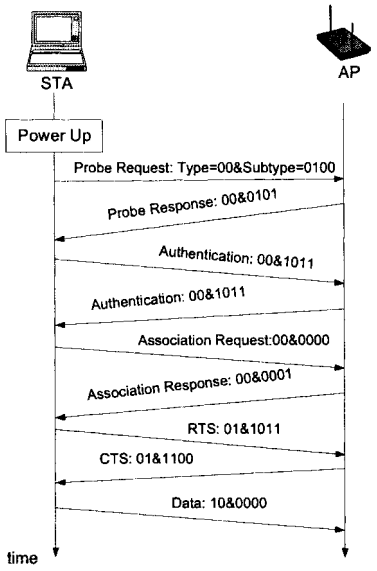

Figure 8.12: An example of MAC frame exchanges between an station and an AP

5. *If the AP accepts the station, an Association Response is sent to the station with the assigned Association ID as well as the supportable rates by the AP.*

6. *If the station has data to send, it first contends the medium with RTS/CTS.*

7. *If the station gains control of the medium, the station starts data transmission.*

8.1.4 Physical layer technologies

Up till now, IEEE has published five physical layer options for 802.11 networks: FHSS and DSSS (802.11) in the 2.4 GHz band, HR-DSSS (802.11b) in the 2.4 GHz band, Further Higher Data Rate Physical Layer Extension in the 2.4 GHz band and OFDM (802.11a) in the 5 GHz band. Please refer to Table 8.1 for their comparisons. Currently, 802.11 Task Group n is working on the future wireless LAN physical layer specifications. Many updated communication technologies, e.g., MIMO, LDPC coding, space-time code, are to be finalized into the standard.

Generally speaking, the 802.11 physical layer is comprised of two sublayers: physical layer convergence procedure (PLCP) and physical medium dependent (PMD) as shown in Figure 8.13. However, the detailed specifications of PLCP and PMD are dependent on the individual PHY option. PLCP defines the

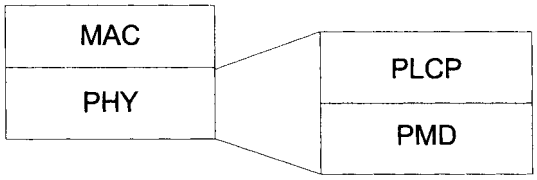

Figure 8.13: Physical layer procedures

method of mapping the MAC PDU (MPDU) onto the framing format that is suitable for the associated PMD transmissions/reception. PLCP thus provides a means to minimize the interaction of the MAC layer with the actual physical operation. PMD defines the characteristics and method of transmitting and receiving data between two stations. It provides the actual means of transmitting and receiving data using the specific PHY scheme. Since this book is centered around OFDM technologies, we focus on 802.11a, which uses OFDM in the physical layer.

In 802.11a, when an MPDU is handed from the MAC layer to the physical layer, PLCP first processes the MPDU to form the physical layer PDU (PPDU) described as follows. A PLCP preamble and a PLCP header are added in front of the MPDU. A Tail field and a Pad field are appended after the MPDU. The PLCP preamble and header are used to aid the demodulation/decoding and delivery of the MPDU at the receiver side. On the other direction, when a PLCP receives a PPDU, it processes the PLCP header to decode the embedded MPDU. The decoded MPDU is then delivered to the MAC layer.

Each PPDU is made up with three parts: Preamble, SIGNAL and DATA. The SIGNAL field is also a part of the PLCP header as shown in Figure 8.14.

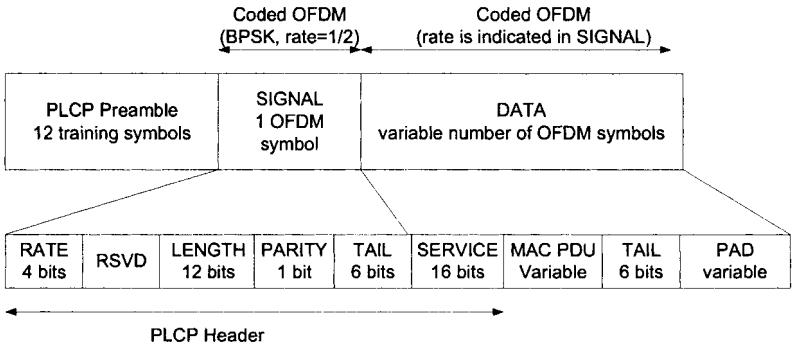

Figure 8.14: 802.11a PLCP frame format

- PLCP Preamble

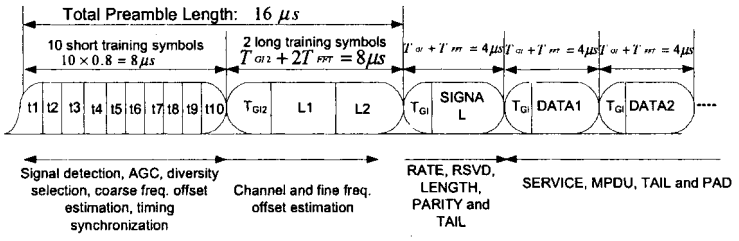

Figure 8.15: 802.11a OFDM training sequence structure

PLCP Preamble contains 10 short training symbols and two long training symbols. The short symbols are used for signal detection, automatic gain control, diversity selection, coarse frequency offset estimation and timing synchronization. The long symbols are used for channel and fine frequency offset estimation. The structure of the training symbols is shown in Figure 8.15.

- The related parameters in Figure 8.15 are defined in Table. 8.3

Parameter	Value
Number of data subcarrier	48
Number of pilot subcarrier	4
Subcarrier frequency spacing ΔF	0.3125 $(20M/64)$
1IFFT/FFT Period T_{FFT}	$3.2\mu s$ $(\frac{1}{\Delta F})$
PLCP Preamble duration $T_{preamble}$	$16\mu s$
Guard duration T_{GI}	$0.8\mu s$ $(\frac{T_{FFT}}{4})$
Long training symbol guard duration T_{GI2}	$1.6\mu s$ $(\frac{T_{FFT}}{2})$
Symbol interval T_{sym}	$4\mu s$ $(T_{GI} + T_{FFT})$

Table 8.3: Timing dependent parameters

One OFDM symbol is transmitted across 52 subcarriers. Four of them are pilots and the remaining 48 carry data. A general OFDM symbol has a 0.8 μs guard interval followed by 3.2 μs data duration. For the long training symbols, the guard interval is 1.6 μs. The frequency domain of the short training sequence is shown in Table 8.4: the short sequence is transmitted on 12 out the 52 subcarriers. In order to normalize the average transmitted power on each subcarrier, a normalizing factor multiplies the short training sequence, i.e.,

$$K_{norm} \times \left(12 \times (1^2 + 1^2)/52\right) = 1.$$

#	Re(·) $\times\sqrt{\frac{13}{6}}$	Im(·) $\times\sqrt{\frac{13}{6}}$	#	Re(·) $\times\sqrt{\frac{13}{6}}$	Im(·) $\times\sqrt{\frac{13}{6}}$	#	Re(·) $\times\sqrt{\frac{13}{6}}$	Im(·) $\times\sqrt{\frac{13}{6}}$
−32	0	0	−10	0	0	12	1	$-j$
−31	0	0	−9	0	0	13	0	0
−30	0	0	−8	−1	$-j$	14	0	0
−29	0	0	−7	0	0	15	0	0
−28	0	0	−6	0	0	16	−1	$-j$
−27	0	0	−5	0	0	17	0	0
−26	0	0	−4	1	$-j$	18	0	0
−25	0	0	−3	0	0	19	0	0
−24	1	j	−2	0	0	20	−1	j
−23	0	0	−1	0	0	21	0	0
−22	0	0	0	0	0	22	0	0
−21	0	0	1	0	0	23	0	0
−20	−1	j	2	0	0	24	1	j
−19	0	0	3	0	0	25	0	0
−18	0	0	4	1	$-j$	26	0	0
−17	0	0	5	0	0	27	0	0
−16	−1	$-j$	6	0	0	28	0	0
−15	0	0	7	0	0	29	0	0
−14	0	0	8	−1	$-j$	30	0	0
−13	0	0	9	0	0	31	0	0
−12	1	$-j$	10	0	0	–	–	–
−11	0	0	11	0	0	–	–	–

Table 8.4: Short training sequence represented in frequency domain

As a result, $K_{norm} = \sqrt{13/6}$.

The long training sequence is transmitted across 53 subcarriers, including a zero value at dc. The frequency domain representation of the long training sequence is shown in Table 8.5.

- SIGNAL field

  SIGNAL field is comprised of RATE, RSVD, LENGTH, PARITY AND SIGNAL TAIL fields as shown in Figure 8.14.

  - RATE field indicates the current data rate. Tables 8.6 shows the encoding of each supportable data rate. The rate-dependent parameters are listed in Table 8.7.

    The data rate is calculated as the number of data bits per OFDM symbol divided by one OFDM symbol interval . For example, 6Mbps is calculated as 24 bits/4μs = 6 Mbps.

  - LENGTH field is the number of bits in the MPDU.

#	Re(·) $\times\sqrt{\frac{13}{6}}$	Im(·) $\times\sqrt{\frac{13}{6}}$	#	Re(·) $\times\sqrt{\frac{13}{6}}$	Im(·) $\times\sqrt{\frac{13}{6}}$	#	Re(·) $\times\sqrt{\frac{13}{6}}$	Im(·) $\times\sqrt{\frac{13}{6}}$
−32	0	0	−10	−1	0	12	−1	0
−31	0	0	−9	1	0	13	−1	0
−30	0	0	−8	1	0	14	−1	0
−29	0	0	−7	−1	0	15	1	0
−28	0	0	−6	1	0	16	1	0
−27	0	0	−5	−1	0	17	−1	0
−26	1	0	−4	1	0	18	−1	0
−25	1	0	−3	1	0	19	1	0
−24	−1	0	−2	1	0	20	−1	0
−23	−1	0	−1	1	0	21	1	0
−22	1	0	0	0	0	22	−1	0
−21	1	0	1	1	0	23	1	0
−20	−1	0	2	−1	0	24	1	0
−19	1	0	3	−1	0	25	1	0
−18	−1	0	4	1	0	26	1	0
−17	1	0	5	1	0	27	1	0
−16	1	0	6	−1	0	28	1	0
−15	1	0	7	1	0	29	1	0
−14	1	0	8	−1	0	30	1	0
−13	1	0	9	1	0	31	1	0
−12	1	0	10	−1	0	–	–	–
−11	−1	0	11	−1	0	–	–	–

Table 8.5: Long training sequence represented in frequency domain

  - RSVD bit is reserved for future use
  - PARITY is an even parity bit for the first 16 bits
  - SIGNAL TAIL shall be set to all zeros.

- DATA

  DATA field is comprised of SERVICE, MPDU, TAIL and PAD fields as shown in Figure 8.14.

  - SERVICE field is also the last field in the PLCP header. The first 6 bits of SERVICE are set to zero to synchronize with the descrambler at the receiver side. The rest of the SERVICE bits are reserved for future use and are also set to zero.
  - MPDU contains the actual information intended to transmit/receive by the stations. It contains the MAC frames constructed according to MAC framing format.
  - TAIL bits are all zeros in order to initialize the convolutional encoder.

Data Rate (Mbps)	Bits
6	1101
9	1111
12	0101
18	0111
24	1001
36	1011
48	0001
54	0011

Table 8.6: SIGNAL field content

Data Rate (Mbps)	Modulation	Coding Rate	Coded Bits per Subcarrier	Coded Bits per OFDM Symbol	Data Bits per OFDM Symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16QAM	1/2	4	192	96
36	16QAM	3/4	4	192	144
48	64QAM	2/3	6	288	192
54	64QAM	2/4	6	288	216

Table 8.7: Rate dependent parameters

  - PAD field contains a variable number of zero bits. It is used to pad the DATA filed into an integral number of OFDM symbols.

- The DATA field including SERVICE, PSDU, TAIL and PAD shall be scrambled with a length-127 frame-synchronous scrambler shown in Figure 8.16. The same scrambler is used to scramble the transmitted bits and descramble the received bits.

  The scrambled bits are then passed into the convolutional encoder shown in Figure 8.17. The coded bits are interleaved and mapped to modulation symbols using BPSK, QPSK, 16-QAM or 64-QAM depending on the rate requested. IFFT/FFT is then implemented and cyclic prefix is added.

  Note that in order to achieve the same average power for all modulation types, a normalizing factor multiplies each symbol. The normalizing factor depends on the modulation type and is shown in Table 8.8.

- Let us take BSPK and 16-QAM as an example of calculating the normalizing factor. The modulated signals for BPSK and 16-QAM are shown in Figure 8.18.

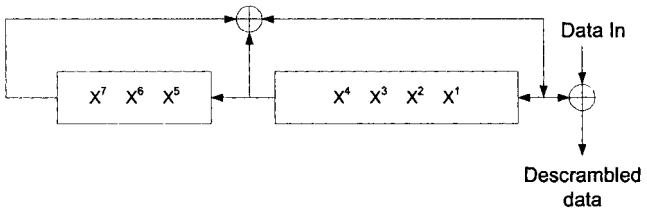

Figure 8.16: 802.11a DATA scrambler/descrambler structure

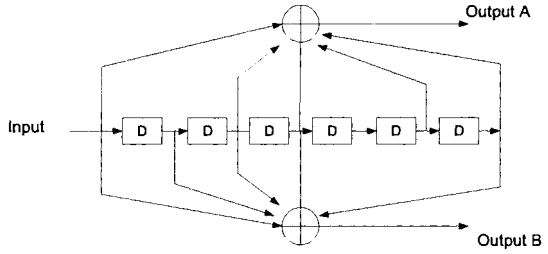

Figure 8.17: 802.11a convolutional encoder

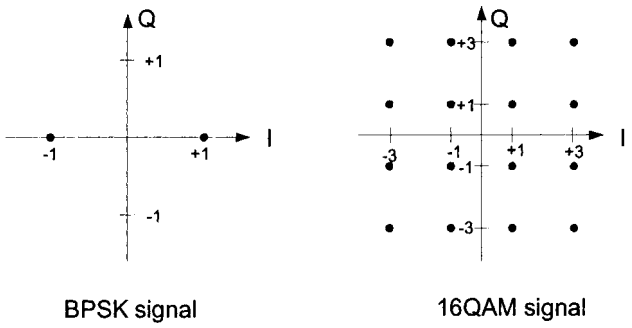

Figure 8.18: QPSK and 16-QAM modulated signals

Modulation	Normalizing Factor K_{MOD}
BPSK	1
QPSK	$1/\sqrt{2}$
16-QAM	$1/\sqrt{10}$
64-QAM	$1/\sqrt{42}$

Table 8.8: Modulation-dependent normalizing factor

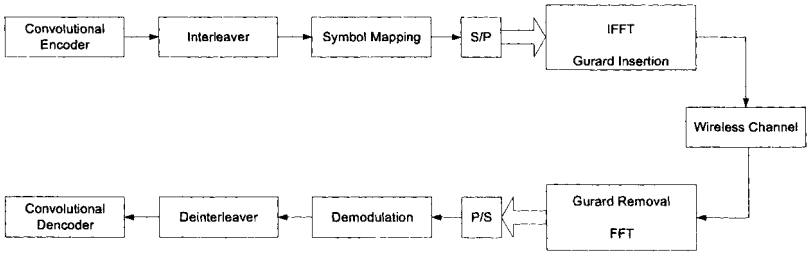

Figure 8.19: 802.11a PHY baseband transmitter and receiver blocks

The average received power for the BPSK signal is calculated as

$$P_{BPSK} = K_{BPSK} \times \frac{1}{2}\left(1^2 + 1^2\right). \tag{8.1}$$

The average received power for the 16-QAM signal is calculated as

$$P_{16-QAM} = K_{16-QAM} \times \frac{1}{16}\left(\begin{array}{c} 4 \times \left(1^2 + 1^2\right) + 4 \times \left(1^2 + 3^2\right) \\ +4 \times \left(3^2 + 1^2\right) + 4 \times \left(3^2 + 3^2\right) \end{array} \right). \tag{8.2}$$

In order for (8.1) and (8.2) to be equal, the normalizing factor should have the following relationship:

$$K_{16-QAM} = \frac{K_{BPSK}}{\sqrt{10}}.$$

Finally, we summarize the 802.11a baseband transmitter and receiver in Figure 8.19.

8.2 IEEE 802.16e and Mobile WiMAX

The IEEE 802.16e is a suite of broadband wireless technologies that are complementary to IEEE 802.11 WiFi. In particular, the IEEE 802.16e standard