IEEE 802.11 Tutorial

Mustafa Ergen
ergen@eecs.berkeley.edu
University of California Berkeley
June 2002

Abstract

This document describes *IEEE 802.11 Wireless Local Area Network (WLAN)* Standard. It describes IEEE 802.11 MAC Layer in detail and It briefly mentions IEEE 802.11a, IEEE 802.11b physical layer standard and IEEE 802.11e MAC layer standard.

Contents

Chapter 1

Overview

1.1 Introduction

- In 1997, the IEEE adopted the first standard for WLANs and revised in 1999.
- IEEE defines a MAC sublayer, MAC management protocols and services, and three physical (PHY) layers.
- PHY Layers:
  1. IR at baseband with 1-2 Mbps,
  2. FHSS at 2.4GHz with 1-2 Mbps,
  3. DSSS at DSSS with 1-2 Mbps.
- IEEE 802.11a ; PHY Layer - OFDM at UNII bands with 54 Mbps
- IEEE 802.11b ; PHY Layer - DSSS at 2.4 GHz with 11Mbps

1.1.1 Goals

- to deliver services previously found only in wired networks.
- high throughput
- highly reliable data delivery
- continuous network connection.

1.1.2 Architecture

Architecture is designed to support a network where mobile station is responsible for the decision making. Advantages are

- very tolerant of faults in all of the WLAN equipment.
- eliminates any possible bottlenecks a centralized architecture would introduce.

Architecture has power-saving modes of operation built into the protocol to prolong the battery life of mobile equipment without losing network connectivity.

Components

Station the component that connects to the wireless medium. Supported services are authentication, deauthentication, privacy, and delivery of the data.

Basic Service Set A BSS is a set of stations that communicate with one another. A BSS does not generally refer to a particular area, due to the uncertainties of electromagnetic propagation. When all of the stations int the BSS are mobile stations and there is no connection to a wired network, the BSS is called independent BSS (IBSS). IBSS is typically short-lived network, with a small number of stations, that is created for a particular purpose. When a BSS includes an access point (AP), the BSS is called infrastructure BSS.

When there is a AP, If one mobile station in the BSS must communicate with another mobile station, the communication is sent first to the AP and then from the AP to the other mobile station. This consume twice the bandwidth that the same communication. While this appears to be a significant cost, the benefits provided by the AP far outweigh this cost. One of them is, AP buffers the traffic of mobile while that station is operating in a very low power state.

Extended Service Set (ESS) A ESS is a set of infrastructure BSSs, where the APs communicate among themselves to forward traffic from one BSS to another and to facilitate the movement of mobile stations from one BSS to another. The APs perform this communication via an abstract medium called the distribution system (DS). To network equipment outside of the ESS, the ESS and all of its mobile stations appears to be a single MAC-layer network where all stations are physically stationary. Thus, the ESS hides the mobility of the mobile stations from everything outside the ESS.

Distribution System the distribution system (DS) is the mechanism by which one AP communicates with another to exchange frames for stations in their BSSs, forward frames to follow mobile stations from one BSS to another, and exchange frames with wired network.

Services

- Station Services: Authentication, De-authentication, privacy, delivery of data
- Distribution Services: Association, Disassociation, Reassociation, Distribution, Integration

Station Services Similar functions to those that are expected of a wired network. The wired network function of physically connecting to the network cable is similar to the authentication and de-authentication services. Privacy is for data security. Data delivery is the reliable delivery of data frames from the MAC in one station to the MAC in one or more other station, with minimal duplication and minimal ordering.

Distribution Services provide services necessary to allow mobile stations to roam freely within an ESS and allow an IEEE 802.11 WLAN to connect with the wired LAN infrastructure. A thin layer between MAC and LLC sublayer that are invoked to determine how to forward frames within the IEEE 802.11 WLAN and also how to deliver frames from the IEEE 802.11 WLAN to network destinations outside of the WLAN.

- The association service makes a logical connection between a mobile station and an AP. It is necessary for DS to know where and how to deliver data to the mobile station. the logical connection is also necessary for the AP to accept data frames from the mobile station and to allocate resources to support the mobile station. The association service is invoked once, when the mobile station enters the WLAN for the first time, after the application of power or when rediscovering the WLAN after being out of touch for a time.
- The reassociation service includes information about the AP with which a mobile station has been previously associated. Mobile station uses repeatedly as it moves in ESS and by using reassociation service, a mobile station provides information to the AP with which the mobile station was previously associated, to obtain frames.
- The disassociation service is used to force a mobile station to associate or to inform mobile station AP is no longer available. A mobile may also use the disassociation service when it no longer require the services of the AP.
- An AP to determine how to deliver the frames it receives uses the distribution service. AP invoke the distribution service to determine if the frame should be sent back into its own BSS, for delivery to a mobile station that is associated with the AP, or if the frame should be sent into the DS for delivery to another mobile station associated with a different AP or to a network destination.
- The integration service connects the IEEE 802.11 WLAN to other LANs, The integration service translates IEEE 802.11 frames to frames that may traverse another network, and vice versa.

Interaction between Some Services The IEEE 802.11 standard states that each station must maintain two variables that are dependent on the authentication, de-authentication services and the association, reassociation, disassociation services. The variables are authentication state and association state and used in a simple state machine that determines the order in which certain services must be invoked and when a station may begin using the data delivery service. A station may be authenticated with many different stations simultaneously. However, a station may be associated with only one other station at a time.

In state 1, the station may use a very limited number of frame types. This frames are to find an IEEE 802.11 WLAN, an ESS, and its APs, to complete the required frame handshake protocols, and to implement the authentication service. If a station is part of an IBSS, it is allowed to implement the data service in state 1. In state2, additional frame types are allowed to provide the capability for a station in state 2 to implement the association, reassociation, and disassociation services. In state 3, all frame types are allowed and the station may use the data delivery service. A station must react to frames it receives in each of the states, even those that are disallowed for a particular state. A station will send a deauthentication notification to any station with which it is not authenticated if it receives frames that are not allowed in state 1. A station will send a disassociation notification to any station with which it is authenticated, but not associated, if it receives frames not allowed in state 2. These notifications will force the station that sent the disallowed frames to make a transition to the proper state in the state diagram and allow it to proceeed properly toward state 3.

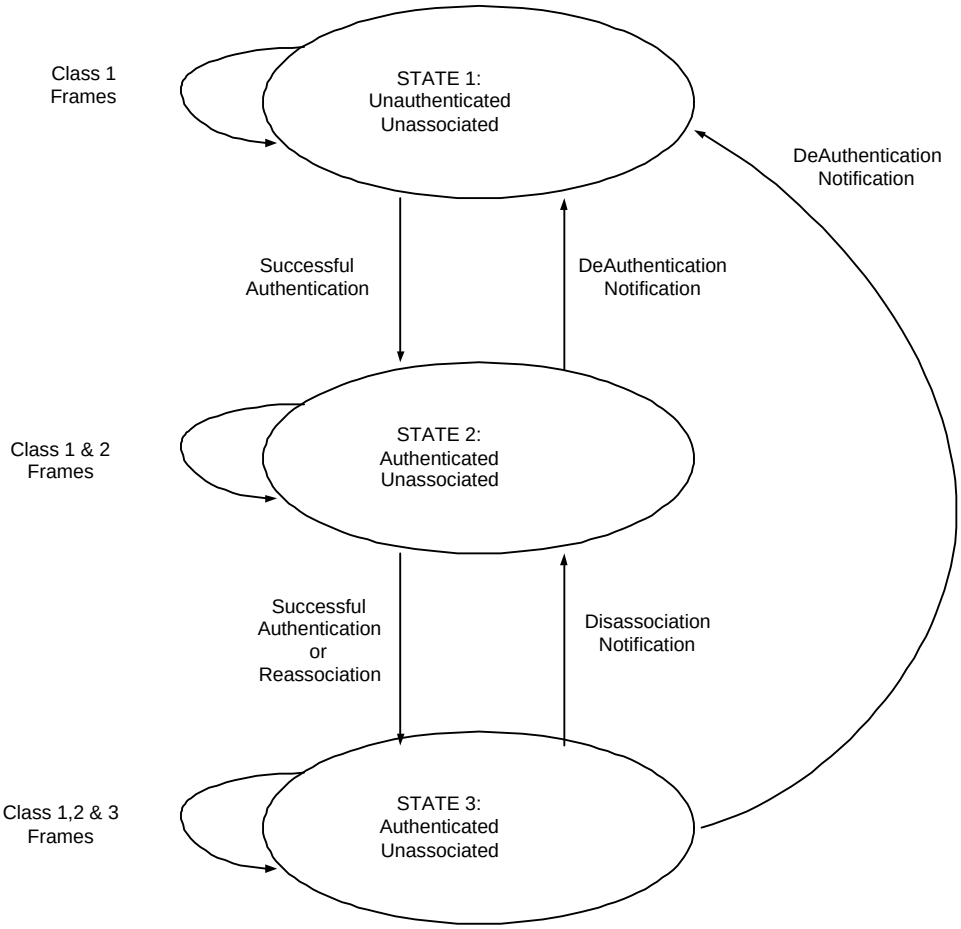
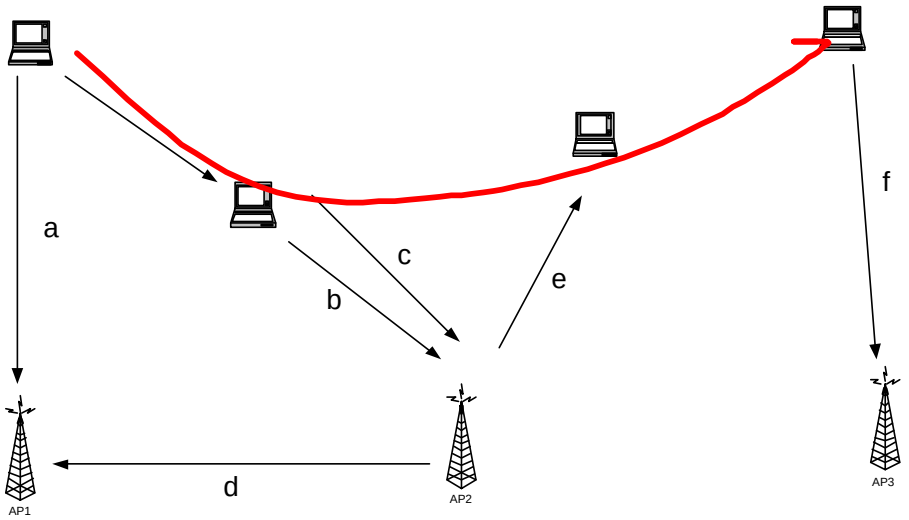


Figure 1.1: Relationship between State Variables and Services



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

Figure 1.2: Relationship between State Variables and Services

Chapter 2

Medium Access Control

MAC protocol supplies the functionality required to provide a reliable delivery mechanism for user data over noisy, unreliable wireless media.

2.1 MAC Functionality

- reliable data delivery
- fairly control access to the shared wireless medium.
- protect the data that it delivers.

2.2 MAC Frame Exchange Protocol

- noisy and unreliable medium
- frame exchange protocol
- adds overhead to IEEE 802.3
- hidden node problem
- requires participation of all stations.
- every station reacts to every frame it receives.

2.2.1 Dealing with Media

The minimal MAC frame exchange protocol consists of two frames, a frame sent from the source to the destination and an acknowledgment from the destination that the frame was received correctly. if the source does not get acknowledgement, it tries to transmit according to the basic access mechanism described below. This reduces the inherent error rate of the medium, at the expense of additional bandwidth consumption without needing higher layer protocols. Since higher layer timeouts are often measured in seconds, it is much more efficient to deal with this issue at the MAC layer.

2.2.2 The Hidden Node Problem

A problem that does not occur on a wired LAN. According to their transmission ranges; A and C can not hear each other and if they transmit at the same time to B, their frames could be corrupted.

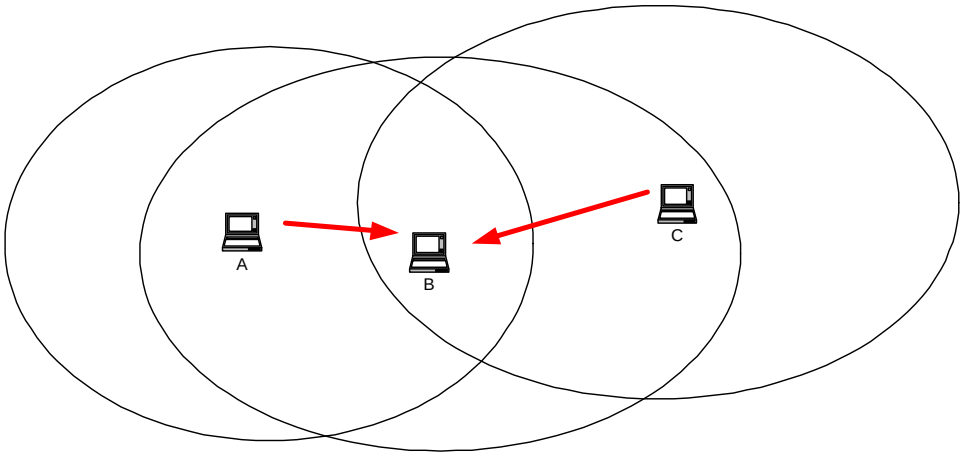


Figure 2.1: The Hidden Node Problem

IEEE 802.11 MAC frame exchange protocol addresses this problem by adding two additional frames to the minimal frame exchange protocol described so far. The two frames are a request to send (RTS) frame and a clear to send (CTS) frame. Source sends RTS and destination replies with CTS and nodes that here RTS and CTS suspends transmission for a specified time indicated in the RTS/CTS frames. See Figure 2.2. These frames are atomic unit of the MAC protocol. Stations that hear RTS delay transmitting until CTS frame. It does not hear CTS, it transmits and The stations that here CTS suspend transmission until they hear acknowledgement.

In the source station, a failure of the frame exchange protocol causes the frame to be retransmitted. This is treated as a collision, and the rules for scheduling the retransmission are described in the section on the basic access mechanism. To prevent the MAC from being monopolized attempting to deliver a single frame, there are retry counters and timers to limit the lifetime of a frame.

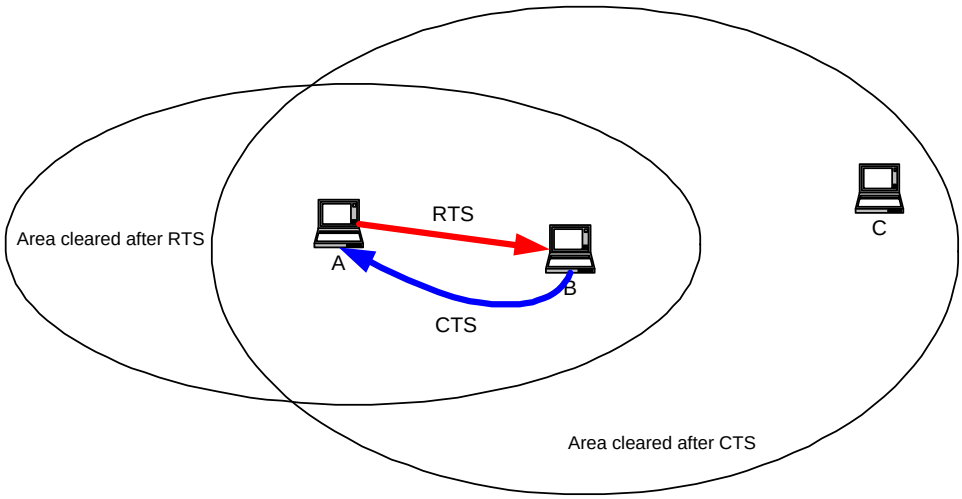


Figure 2.2: RTS and CTS address the Hidden Node Problem

RTS/CTS mechanism can be disabled by an attribute in the management information base (MIB). The value of the *dot11RTSThreshold* attribute defines the length of a frame that is required to be preceded by the request to send and clear to send frames.

Where RTS/CTS can be disabled;

- low demand for bandwidth
- where the stations are concentrated in an area where all area where all are able to hear the transmissions of every station.
- where there is not much contention for the channel.

Default value of the threshold is 128 and by definition, an AP is heard by all stations in its BSS and will never be a hidden node. When AP is colocated and sharing a channel, the value for the RTS can be changed.

2.2.3 Retry Counters

Two retry counters associated with every frame the MAC attempts to transmit: a short retry counter and a long retry counter. There is also a lifetime timer associated with every frame the MAC attempts to transmit. Between these counters and the timer, the MAC may determine that it may cancel the frame‘s transmission and discard the frame. Then MAC indicates to the MAC user through the MAC service interface. Fewer tries for the shorter frames as compared to longer frames which is determined from the value of an attribute in the MIB, *dot11RTSThreshold*. These counters are incremented in each unsuccessful transmission. When they reach the limit associated in MIB(*dot11ShortRetryLimit, dot11LongRetryLimit*) they are discarded.

2.2.4 Basic Access Mechanism

The basic access mechanism is carrier sense multiple access with collision avoidance (CSMA/CA) with binary exponential backoff similar to IEEE 802.3, with some significant exceptions. CSMA/CA is a "listen before talk" (LBT) access mechanism. When there is a transmission in the medium, the station will not begin its own transmission. This is the CSMA portion of the access mechanism. If there is a collision and the transmission corrupted, the operation of the access mechanism works to ensure the correct reception of the information transmitted on the wireless medium.

As IEEE 802.11 implements this access mechanism, when a station listens to the medium before beginning its own transmission and detects an existing transmission in progress, the listening station enters a wait period determined by the binary exponential backoff algorithm. It will also increment the appropriate retry counter associated with the frame. The binary exponential backoff mechanism chooses a random number which represents the amount of time that must elapse while there are not any transmissions, i.e., the medium is idle before the listening station may attempt to begin its transmission again. The random number resulting from this algorithm is uniformly distributed in a range, called the *contention window*, the size of which doubles with every attempt to transmit that is deferred, until a maximum size is reached for the range. Once a transmission is successfully transmitted, the range is reduced to its minimum value for the next transmission.

It is extremely unusual for a wireless device to be able to receive and transmit simultaneously, the IEEE 802.11 MAC uses collision avoidance rather than the collision detection of IEEE 802.3. It is also unusual for all wireless devices in LAN to be able to communicate directly with all other devices. For this reason, IEEE 802.11 MAC implements a network allocation vector (NAV). The NAV is a value that indicates to a station the amount of time that remains before the medium will become available. Even if the medium does not appear to be carrying a transmission by the physical carrier sense, the station may avoid transmitting. The NAV, then, is a virtual carrier sensing mechanism. By combining the virtual carrier sensing mechanism with the physical carrier sensing mechanism, the MAC implements the collision avoidance portion of the CSMA/CA access mechanism.

2.2.5 Timing Intervals

There are five timing intervals.

1. PHY determines: the short interframe space (SIFS)
2. PHY determines: the slot time.
3. the priority interframe space (PIFS),
4. the distributed interframe space (DIFS),
5. and the extended interframe space (EIFS).

The SIFS is the shortest interval, followed by the slot time which is slightly longer. The PIFS is equal to SIFS plus one slot time. The DIFS is equal to the SIFS plus two slot times. The EIFS is much larger than

any of the other intervals. It is used when a frame that contains errors is received by the MAC, allowing the possibility for the MAC frame exchanges to complete correctly before another transmission is allowed. Through these five timing intervals, both the DCF and PCF are implemented.

2.2.6 DCF Operation

The basic 802.11 MAC protocol is the DCF based on CSMA. Stations deliver *MAC Service Data Units* (MSDUs). Stations deliver MSDUs of arbitrary lengths up to 2304 bytes, after detecting that there is no other transmission in progress on the channel. However, if two stations detect the channel as free at the same time, a collision occurs. The 802.11 defines a *Collision Avoidance (CA)* mechanism to reduce the probability of such collisions. Before starting a transmission a station has to keep sensing the channel for an additional random time after detecting the channel as being idle for a minimum duration called DIFS, which is 34 *us* for the 802.11a PHY. Only if the channel remains idle for this additional random time period, the station is allowed to initiate its transmission.

1. when the MAC receives a request to transmit a frame, a check is made of the physical and virtual carrier sense mechanisms.
2. if the medium is not in use for an interval of DIFS (or EIFS if the pre-received frame is contained errors), the MAC may begin transmission to the frame.
3. if the medium is in use during the DIFS interval, the MAC will select a backoff and increment the retry counter.
4. The MAC will decrement the backoff value each time the medium is detected to be idle for an interval of one slot time.
5. it there is a collision, the contention window is doubled, a new backoff interval is selected.

An example of a DCF operation is seen in Figure 2.3.

2.2.7 Centrally Controlled Access Mechanism

Uses a poll and response protocol to eliminate the possibility of contention for the medium. This access mechanism is called PCF. A point coordinator (PC) controls the PCF. The PC is always located in an AP. Generally, the PCF operates by stations requesting that the PC register them on a polling list, and the PC then regularly polls the stations for traffic while also delivering traffic to the stations. The PCF is built over the DCF and both operate simultaneously. The PCF uses PIFS instead of DIFS. The PC begins a period of operation called the contention-free period (CFP), during which the PCF is operating. This period is called contention free because access to the medium is completely controlled by the PC and the DCF is prevented from gaining access to the medium. The CFP occurs periodically to provide a near-isochronous service to the stations. The CFP also alternates with a contention period where the normal DCF rules operate and all

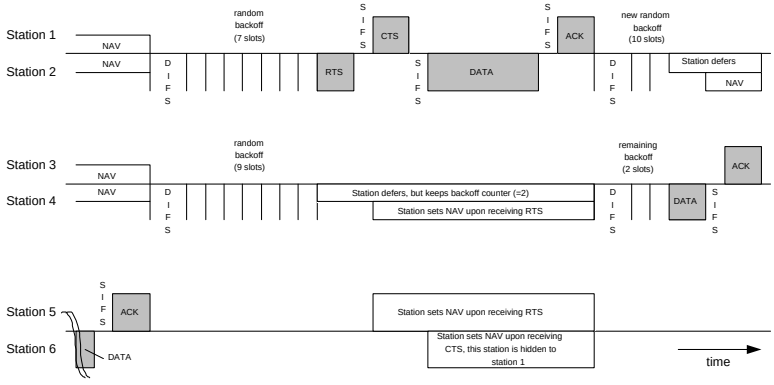


Figure 2.3: Timing of the 802.11 DCF. In this example, station 6 cannot detect the RTS frame of the transmitting station 2, but the CTS frame of station 1.

stations may compete for access to the medium. The standard requires that the contention period be long enough to contain at least one maximum length frame and its acknowledgement.

The CFP begins when the PC gains access to the medium, using the normal DCF procedures, and transmits a Beacon frame. Beacon frames are required to be transmitted periodically for PC to compete for the medium. The traffic in the CFP will consists of frames sent from the PC to one or more stations, followed by the acknowledgement from those stations. In addition, PC sends a contention-free-poll (CF-Poll) frame to those stations that have requested contention-free service. If the station has data to send then respond to CF-Poll. For medium efficient utilization, it is possible to piggyback both the acknowledgement and the CF-Poll onto data frames.

During the CFP, the PC ensures that the interval between frames to the medium is no longer than PIFS to prevent a station operating under the DCF from gaining access to the medium. Until CFP, PC sends in SIFS and waits for response for SIFS and tries again.

NAV prevents stations from accessing the medium during the CFP. Beacon contains the information about maximum expected length of the CFP. The use of PIFS for those who did not receive beacon. PC announces the end of the CFP by transmitting a contention-free end (CF-End) Frame. It resets NAV and stations begin operation of DCF, independently.

There are problems with the PCF that led to the current activities to enhance the protocol. Among many others, those include the unpredictable beacon delays and unknown transmission durations of the polled stations. At TBTT target beacon transmission time (TBTT), a PC schedules the beacon as the next frame to be transmitted, and the beacon can be transmitted when the medium has been determined to be idle for at least PIFS. Depending on the wireless medium at this point of time, i.e., whether it is idle or busy around the TBTT, a delay of the beacon frame may occur. The time the beacon frame is delayed, i.e., the duration it is sent after the TBTT, delays the transmission of time-bounded MSDUs that have to be delivered in CFP. From the legacy 802.11 standard, stations can start their transmissions even if the MSDU Delivery cannot finish before the upcoming TBTT [3]. This may severely affect the QoS as this introduces unpredictable time

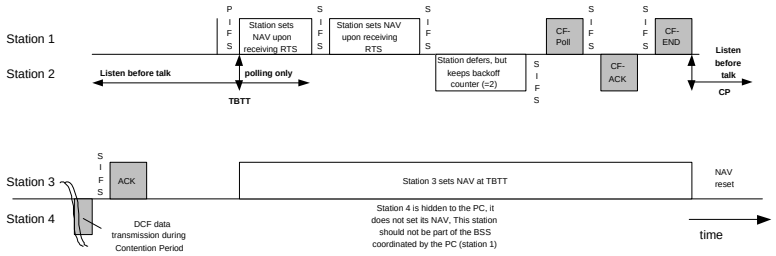


Figure 2.4: Example for the PCF operation. Station 1 is the PC polling station 2. Station 3 detects the beacon frame and sets the NAV for the whole CFP. Station 4 is hidden to station 1 and does not detect the beacon frame; it continues to operate in DCF.

delays in each CFP. Beacon frame delays of around 4.9ms are possible in 802.11a in the worst case.

2.2.8 Frame Types

MAC accepts MSDUs from higher layers and add headers and trailers to create MPDU. The MAC may fragment MSDUs into several frames, increasing the probability of each individual frame being delivered successfully. Header+MSDU+Trailer contains information;

- addressing information
- IEEE 802.11-specific protocol information
- information for setting the NAV
- frame check sequence for verifying the integrity of the frame.

General Frame Format

FC	D/ID	Addr. 1	Addr. 2	Addr. 3	Seq Cont.	Addr. 4	Data	FCS	
2	2	6	6	6	2	6	0-2312	4	bytes

FC - Frame Control: 16bits

1. Protocol Version: 2 bits; to identify the version of the IEEE 802.11 MAC protocol: set to zero now.
2. Frame Type and Sub Type: identifies the function of the frame and which other MAC header fields are present in the frame. Within each frame types there may be subparts.
3. To DS and From DS: To DS is 1bit length; Set every data sent from mobile station to the AP. Zero for all other frames. From DS is 1 bit again and for the data types from AP to the mobiel station. When both zero that means a direct communication between two mobile stations. When both are

on, for special case where an IEEE 802.11 WLAN is being used as the DS refeered as wireless DS. The frame is being sent from one AP to another, over the wireless medium.

4. More Fragments Subfield: 1bit; indicates that this frame is not the last fragment of a data or management frame.
5. Retry Subfield: 1bit; when zero, the frame is transmitted for the first time, otherwise it is a retransmission.
6. Power Management Subfield: 1bit;mobile station announces its power management state; 0 means station is in active mode and 1 means the station will enter the power management mode. The subfield should be same during the frame exchange in order for the mobile to change its power management mode. Frame exchange is 2or 4 way frame handshake including the ACK.
7. More Data Subfield: 1bit; AP uses to indicate to a mobile station that there is at least one frame buffered at the AP for the mobile station. Mobile polled by the PC during a CFP also may use this subfield to indicate to the PC that there is at least one more frame buffered at the mobile station to be sent to the PC. In multicast , AP may also set to indicate there are more multicast frames.
8. WEP Subfield: 1bit; 1 indicates that the frame body of MAC frame has been encrypted using WEP algorithm.(only data and management frames os subtype authentication)
9. Order Subfield: 1bit; indicates that the content of the data frame was provided to the MAC with a request for strictly ordered service. provides information to the AP and DS to allow this service to be delivered.

Duration/ID Field (D/ID): 16bits; alternatively contains information for NAV or a short ID(association ID-AID)used mobile station to get its buffered frames at the AP. only power-save poll (PS-Poll) frame contains the AID. most two significant bit is set to 1 and the rest contains ID. All values larger than 2007 are reserved.

When 15bit is zero the rest (14-0) represents the remaining duration of a frame exchange to update NAV. The value is set to 32,768(15bit=1 and the rest 0) in all frames transmitted during the CFP to allow a station who missed the beginning to recognize that it is in middle of the CFP session and it set NAV a higher value.

Address Fields: 4 address fields: besides 48bit address (IEEE 802.3) additional address fields are used (TA,RA,BSSID) to filter multicast frames to allow transparent mobility in IEEE 802.11.

1. IEEE 48bit address comprises three fields:
   - a single-bit Individual/Group field: When set to 1, the address is that of a group. if all bit are 1 , that means broadcast.
   - a single-bit Universal/Local bit; when zero, the address is global and unique, otherwise it may no be unique and locally administered.
   - 46bit address fields.

2. BSS Identifier (BSSID): unique identifier for a particular BSS. In an infrastructure BSSID it is the MAC address of the AP. In IBSS, it is random and locally administered by the starting station. This also give uniqueness. In the probe request frame and group address can be used.
3. Transmitter Address (TA): MAC address of the station that transmit the frame to the wireless medium. Always an individual address.
4. Receiver Address (RA): to which the frame is sent over wireless medium. Individual or Group.
5. Source Address (SA): MAC address of the station who originated the frame. Always individual address. May not match TA because of the indirection performed by DS of an IEEE 802.11 WLAN. SA field is considered by higher layers.
6. Destination Address (DA): Final destination . Individual or Group. May not match RA because of the indirection.

Sequence Control Field: 16bit: 4bit fragment number and 12bit sequence number. Allow receiving station to eliminate duplicate received frames.

1. Sequence Number Subfield: 12bit; Each MSDU has a sequence number and it is constant. Sequentially incremented for the following MSDUs.
2. Fragment Number Subfield: 4bits; Assigned to each fragment of an MSDU. The firs fragment is assigned to zero and incremented sequentially.

Frame Body Field: contains the information specific to the particular data or management frames. Variable length. As long as 2304bytes and when ecrypted 2312bytes. An application may sent 2048byte with 256 byte upper layer headers.

Frame Check Sequence Field: 32 bits; CCITT CRC-32 polynomial:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

The frame check sequence is an IEEE 802 LAN standards and generated in the same way as it is in IEEE 802.3.

2.2.9 Control Frame Subtypes

Request to Send 20bytes;

- Frame Control Field:
- Duration/ID field:
- RA-always individual address
- TA

- FCS

The purpose is to transmit the duration to stations in order for them to update their NAV to prevent transmissions from colliding with the data or management frame that is expected to follow. Duration information conveyed by this frame is a measure of the amount of time required to complete the four-way frame exchange. Duration (ms)= CTS+Data or management frame+ ACK+ 2 SIFS

Clear to Send: 14bytes;

- Frame Control Field, Duration/ID Field
- RA, individual MAC address
- FCS

for updating the NAV. Duration (ms) =Data or management frame + ACK + 1 SIFS

Acknowledge: 14 bytes;

- Frame Control Field
- Duration/ID Field (ms): Duration is zero if the ACK is an acknowledgement. The value of the duration information is the time to transmit the subsequent data or management frame, an ACK frame, and two SIFS intervals, if the acknowledgement is of a data or management frame where the more fragments subfield of the frame control field is one.
- RA: individual address. RA is taken from the address 2 field of data, management or PS-Poll frame.
- FCS

The purpose of this frame is two-fold. First, the ACK frame transmits an acknowledgement to the sender of the immediately previous data, management, or PS-Poll frame that the frame was received correctly. Second, the ACK frame is used to transmit the duration of information for a fragment burst as in CTS.

Power Save Poll: 20 bytes;

- Frame Control Field
- Duration/ID Field: AID value given to the mobile station upon association with the BSS. when a PS-Poll frame will update its NAV with a value which is the length of time to transmit an ACK and SIFS interval this action for AP to send ACK.
- BSSID
- TA: MAC address of the mobile station that is sending the PS-Poll Frame.
- FCS

Function	To DS	From DS	Address 1	Address 2	Address 3	Address 4
IBSS	0	0	RA=DA	SA	BSSID	N/A
From the AP	0	1	RA=DA	BSSID	SA	N/A
To the AP	1	0	RA=BSSID	SA	DA	N/A
Wireless DS	1	1	RA	TA	DA	SA

Table 2.1: Address Field Functions

The purpose of this frame is to request that an AP deliver a frame that has been buffered for a mobile station while it was in a power saving mode.

CF-End and CF-End+ACK: 20 bytes;

- Frame Control Field,
- Duration/ID Field: Duration value is zero.
- BSSID: MAC address of the AP
- RA: the broadcast group.

Purpose of these frames is to conclude a CFP and to release stations from the restriction imposed during a CFP. CF-End+ACK frame is used to acknowledge the last transmission received by the PC.

2.2.10 Data Frame Subtypes

Data: Data frame is variable in length (29-2346 bytes). Duration ID field contains a value, measured in microseconds from the end of the frame, sufficient to protect the transmission of a subsequent acknowledgement frame. If the data frame is multicast address, the duration/ID value is zero. Address fields are dependent to the network and identified in table 6.1.

- The address 2 field is used to identify the sender of the frame. This is used in ACK.
- The address 3 field carries additional information for frame filtering or forwarding by the DS. When a mobile station receive a frame by AP, it uses this field as the destination address to indicate the higher layer protocols. A frame received by AP from a mobile station will use this address as the destination address of the frame for DS forwarding decisions. In the wireless DS, it contains the destination address of the frame that was originally received by the AP.
- The address 4 field is used only in a wireless DS as one AP forwards a frame to another AP.The source address of the original AP is contained here.
- DA is the destination of the MSDU in the frame body field.
- SA is the address of the MAC entity that initiated the MSDU in the frame body field.

- RA is the address of the station contained in the AP in the wireless DS that is next recipient.
- TA is the address of the station contained in the AP in the wireless DS that is transmitting the frame.
- BSSID is the address currently in use by the station contained in the AP if the station is AP or is associated with an AP. Otherwise, BSSID is the BSSID of the IBSS.

Data+CF-ACK: Sent only during a CFP. Never used in IBSS. ACK is for previously received data frame, which may not be associated with the address of the destination of the current frame.

Data+CF-Poll: This frame is used only by PC during a CFP to deliver data to a mobile station and simultaneously request that the mobile station send a data frame that it may have buffered, when the current reception is completed.

Data+CF-ACK+CF-Poll: Combines the Data+CF-ACK and Data+CF-Poll frames into a single frame and used by the PC during a CFP.

Null Function (no data): This frame is a data frame with no frame body and used to allow a station that has nothing to transmit to be able to complete the frame exchange necessary for changing its power management state. The sole purpose for this frame is to carry the power management bit in the frame control field to the AP, when a station changes to a low power operating state.

CF-ACK (no data): Mobile station uses to acknowledge the PC during a CFP. ACK is more efficient since this frame is 29bytes long.

CF-Poll (no data): PC uses to request that a mobile station send a pending data frame during the CFP.

CF-ACK+CF-Poll (no data): Used by the PC and combines CF-ACK and CF-Poll .

2.2.11 Management Frame Subtypes

IEEE 802.11 is different from many of the other IEEE 802 standards because it includes very extensive management capabilities defined at the MAC level. One of the four MAC frame types is dedicated to management frames. There are 11 distinct management frame types. All management frames include:

- Frame Control,
- Duration,
- Address 1, 2, and 3,
- Sequence control,
- Framebody,

  - Element ID
  - Length
  - Information (variable length)

- Frame check sequence (FCS) fields.

Beacon: It is used to identify a BSS. The Beacon frame also conveys information to mobile stations about frames that may be buffered during times of low power operation. The Beacon frame includes the following fixed fields:

Timestamp: 64bits, contains the value of the station‘s synchronization timer at the time that the frame was transmitted.

Beacon Interval: 16-bit, The Beacon interval is the period, measured in “time units ” (TU) of 1024 microseconds, of beacon transmissions.

Capability Information: 16-bit, it identifies the capabilities of the station.

The information elements in a Beacon frame are the service set identity (SSID), the supported rates, one or more PHY parameter sets, an optional contention-free parameter set, an optional IBSS paramater set, and an optional traffic indication map.

Probe Request and Response: Mobile station transmits to quickly locate an IEEE 802.11 WLAN. (with a particular SSID or any WLAN). It contains SSID and the supported rates. In the infrastructure BSS, the AP will always respond to probe requests and in IBSS, the mobile station that sent the latest Beacon will respond.

The probe response contains nearly all the same information as a Beacon frame and includes the timestamp, beacon interval, and capability information fixed fields. It also includes the SSID, supported rates, one or more PHY parameter sets, the optional contention-free parameter set, and the optional IBSS parameter set.

Authentication: The authentication frame is used to conduct a multiframe exchange between stations that ultimately results in the verification of the identity of each station to the other, within certain constraints. The authentication frame includes three fixed fields.

- the authentication algorithm number
- the authentication transaction sequence number
- the status code.
- status code.

Deauthentication: The station uses to notify another station of the termination of an authentication relationship. The frame includes only a single fixed field, the reason code.

Association Request and Response: The mobile station request an association with a BSS and for the success or failure of that request is returned to the mobile station by the response. The association request frame includes two fixed fields, the capability information field and the listen interval. There are also two information elements in the association request, the SSID and the supported rates.

The association response frame includes three fixed fields: the capability information, the status code, and the association ID. There is one information element in the association response, the supported rates.

Reassociation Request and Response: Mobile station that has been associated with a BSS and is now associating with another BSS with the same SSID uses the reassociation request that includes the same information as an association request frame, with the addition of a current AP address fixed field. The reassociation response frame is identical to the association response frame.

Disassociation: The station notifies another station of the termination of an association relationship. The frame includes only a single fixed field, the reason code.

Announcement Traffic Indication Message: The announcement traffic indication message (ATIM) frame is used by mobile stations in an IBSS to notify other mobile stations in the IBSS that may have been operating in low power modes that the sender of the ATIM frame has traffic buffered and waiting to be delivered to the station addressed in the ATIM frame.

2.2.12 Components of the Management Frame Body

Fixed Fields

Association ID (AID): 16-bit, It contains an arbitrary number assigned by the AP when a station associates with a BSS. The value is in the least significant 14 bits. The most 2 bit is set to 1.

Authentication Algorithm Number: 16-bit, it contains a number identifying the authentication algorithm to be used to complete an authentication transaction. 0 is for "open system" and 1 is for " shared key" and the rest is reserved for future usage.

Authentication Transaction Sequence Number: 16-bit, It tracks the progress of an authentication transaction. The number is increased sequentially with each authentication frame exchanged during the transaction.

Beacon Interval: 16-bit, It indicates the typical amount of time that elapses between Beacon frame transmissions. One TU (time units) is 1024 μs.

Capability Information: 16-bit,

- ESS
- IBSS

- CF pollable
- CF-Poll request
- privacy.

in IEEE 802.11b additionally three subfields are added.

- short preamble
- PBCC
- channel agility

The ESS and IBSS subfields are significant only in Beacon and probe response frames. AP sets ESS subfield to 1 and the IBSS subfield to 0 and a mobile station in an IBSS always sets the ESS subfield to 0 and the IBSS subfield to 1.

The CF pollable an CF-Poll request subfields are significant in Beacon, probe response, association request, association response, reassociation request, and reassociation response frames. A mobile station will set these subfields in association request and reassociation request frames to indicate its contention-free capability and to request that it be placed on the polling list of the PC.

An AP will set these subfields in Beacon, probe response, association response, and reassociation response frames to indicate the capability of the PC.

The privacy subfield is transmitted by the AP in Beacon, probe response, association response, and reassociation response frames. In addition to indicating that the AP implements WEP, when set to 1, that means WEP is compulsory otherwise optional.

The short preamble subfield if transmitted by an AP or a mobile station in an IBSS in Beacon, probe response, association response, and reassociation response frames to indicate the availability of the short preamble option when using an IEEE 802.11b PHY. When set to 1, short preambles is allowed, when 0, it is not allowed.

The packet binary convolutional coding (PBCC) subfield is transmitted by an AP or a mobile station in an IBSS in Beacon, probe response, association response, and reassociation response frames to indicate the availability of the PBCC option when using an IEEE 802.11b PHY.

When a mobile station is not part of an IBSS, the PBCC subfield in association request and reassociation request frames indicates the capability of the station to send and receive the PBCC of IEEE 802.11b.

The channel agility subfield indicates that the station is using the channel agility option of IEEE 802.11b.

Current AP Address: 6 bytes, It holds the address of the AP with which a mobile station is currently associated, when that mobile station is attempting to reassociate. If the reassociation is successful, the new AP uses that AP address to contact and retrieve frames that may have been buffered there for the mobile station.

Listen Interval: 16-bit, The listen interval is used by a mobile station to indicate to an AP how long the mobile station may be in low power operating modes and unable to receive frames. The value is in units of the Beacon interval.

Reason Code: 16-bit, It indicates the reason for an unsolicited notification of disassociation or deauthentication.

Status Code: 16-bit, It indicates the success or failure of a requested operation.

Timestamp: 64-bit, It is the value of the station‘s TSFTIMER at the time a frame was transmitted.

Information Elements: SSID, Supported rates, FH parameter set, DS parameter set, CF parameter set, TIM, IBSS parameter set, Reserved, Challenge text, Reserved for challenge text extension.

Service Set Identity (SSID) , max 32-bit,: This information carries the SSID of the IEEE 802.11 WLAN. When the length is zero, that means it is broadcasted. The broadcast identity is used in probe request frames when the mobile station is attempting to discover all IEEE 802.11 WLANs in its vicinity.

Supported Rates: 1-8 bytes, Each byte represents a single rate where the lower 7 bits of the byte representing the rate value, and the most significant bit indicating whether the rate is mandatory or not.

The supported rates element is transmitted in Beacon, probe response, association request, association response, reassociation request, and reassociation response frames. If a station does not support all of the rates indicated to be mandatory, it may not associate with the BSS.

FH Parameter Set: 7 bytes, two byte element ID, length, the element contains the dwell time, hop set, hop pattern, and hop index. The FH parameter set element is present in Beacon and probe response frames only if the PHY being used is the IEEE 802.11 FHSS PHY or the IEEE 802.11b PHY with the channel agility option enabled.

DS Parameter Set: 3 bytes, It contains the element ID and length and current channel. This element is present in Beacon and probe response frames only if the IEEE 802.11 DSSS or IEEE 802.11b PHY is being used.

CF Parameter Set: 8 bytes, In addition to the element ID and length, this element contains the CFP count, CFP period, CFP max duration, and CFP duration remaining. This frame is present in Beacon and probe response frames only if a PC is in operation in the BSS.

Traffic Indication Map: 6-256 bytes, This element carries information about frames that are buffered at the AP for stations in power saving modes of operation.

- Element ID
- Length
- Delivery TIM (DTIM) count:

- DTIM period
- bitmap control
- partial virtual bitmap

The DTIM count and DTIM period are used to inform mobile stations when multicast frames that have been buffered at the AP will be delivered and how often that delivery will occur. DTIM count is an integer value that counts down to zero. This value represents the number of Beacon frames that will occur before the delivery of multicast frames. DTIM period is the number of Beacon frames between multicast frame deliveries. The DTIM period has a significant effect on the maximum power savings a station may achieve.

IBSS Parameter Set: it occurs in beacon frames in an IBSS. It contains element ID, length and also the ATIM window field. The announcement TIM (ATIM) window field is 16-bits long and indicates the length of the ATIM window after each Beacon frame transmission in an IBSS. The length of the ATIM window is indicated in TU.

Challenge Text: 255 bytes, In addition to the element ID and length fields, this element carries one more field, the challenge text.

2.2.13 Other MAC Operations

Fragmentation:

The IEEE 802.11 MAC can fragment its frames in an attempt to increase the probability that they will be delivered without errors induced by the interference. When a frame is fragmented, the sequence control field of the frame header indicates the placement of the individual fragment among the set of fragments. The more fragments bit in the frame control field indicates whether the current fragment is the last fragment. The fragments are transmitted in burst and they do not need to compete for the medium again since the medium is reserved for the burst and duration is updated in every fragment and ACK.

Privacy:

The WLAN lacks even the minimal privacy provided by a wired LAN. The IEEE 802.11 Wired Equivalent Privacy (WEP) mechanism provides protection at a level that is felt to be equivalent to that of a wired LAN. Data frames that are encrypted are sent with the WEP bit in the frame control field of the MAC header set. The receiver decrypt the frame and passes to the higher layer protocols.

Only the frame body is encrypted, this leaves the complete MAC header of the data frame, and the entire frame of other frame types, unencrypted and available to even the casual eavesdroppers.

The encryption algorithm used in IEEE 802.11 is RC4 developed by Ron Rivest of RSA Data Security, Inc. RC4 is a symmetric stream cipher that supports a variable key length (IEEE 802.11 chosen 40 bit key length). It is symmetric since the same key and algorithm are used for both encryption and decryption. Unlike

a block chipper that processes a fixed number of bytes, a stream chipper is an algorithm that can process an arbitrary number of bytes.

The IEEE 802.11 standard describes the use of the RC4 algorithm and the key in WEP. However, key distribution or key negotiation is not mentioned in the standard left to the individual manufacturers of IEEE 802.11 equipment. Secure placement of keys int the individual stations is a discussion in IEEE 802.11 working group.

WEP Details:

IEEE 802.11 provides two mechanisms to select a key for use when encrypting or decrypting a frame. The first mechanism is a set of as many as four default keys. Default keys are intended to be shared by all stations in a BSS or an ESS. The benefit of using a default key is that, once the station obtains the default keys, a station can communicate securely with all of the other stations in a BSS or ESS. The problem is they are widely distributed to many stations and may be more likely to be revealed.

The second mechanism provided by IEEE 802.11 allows a station to establish a "key mapping" relationship with another station. Key mapping allows a station to create a key that is used with only one other station.

The *dot11PrivacyInvoked* attribute controls the use of WEP in a station. If it is set false, all frames are sent without encryption. Encryption for specific destinations may only be disabled if a key mapping relationship exists with that destination.

A default key may be used to encrypt a frame only when a key mapping relationship does not exist between the sending and receiving station. A key is available if its entry in the *dot11WEPDefaultKeysTable* is not null. If one or more default keys is available algorithm which is not defined in the standard chooses one of them. The WEP header and trailer are appended to the encrypted frame body, the default key used to encrypt the frame is indicated in the KeyID of the header portion along with the initialization vector, and the integrity check value (ICV) in the trailer.

If key mapping relationship exists between source and destination stations, the "key mapping key," the key shared only by the source and destination stations, must be used to encrypt frames sent to that destination. The key is chosen *dot11WEPKeyMappingsTable*. The frame body is encrypted using the key mapping key, and the WEP header and trailer are appended to the encrypted frame body, If the *dot11WEPKeyMappingWEPOn* entry for the destination is true.

Corresponding to the *dot11PrivacyInvoked* attribute controlling the sending of frames, the *dot11ExcludeUnencrypte* attribute controls the reception of encrypted frames. When it is false, all frames is accepted, whether they are encrypted or not, otherwise only the encrypted ones will be received.

WEP associate with two counters. The *dot11UndecryptableCount* reflects the number of encrypted frames that were received by the station that could not be decrypted. The *dot11ICVErrorCount* reflects the number of frames that were received by a station for which a key was found that resulted in the calculated ICV value not matching the ICV received with the frame. These two counters should be monitored carefully when WEP is used in a WLAN. The *dot11UndecrptableCount* indicates that an attack to deny service may be in progress, if the counter is increasing rapidly. The *dot11ICVErrorCount* can indicate that an attack to determine a key is in progress, if this counter is increasing rapidly.

Chapter 3

MAC Management

Because the media over which the IEEE 802.11 WLAN operate are not wires, the media are shared by other users that have no concept of data communication or sharing the media. An example of this type of user is the common microwave oven. The microwave oven operates in the 2.4 GHz ISM band because one excitation frequency of the water molecule lies in this band. Another user in this same band is the radio frequency ID (RFID) tag. RFID tags are usually small, cheap, unpowered devices that receive their power from a microwave beam and then return a unique identifier. RFID tags are used to track retail inventory, identify rail cars, and many other uses.

There are also other WLANs than IEEE 802.11 that share the media. This would be somewhat equivalent to attempting to run IEEE 802.3, IEEE 802.5, IEEE 802.12, and fiber distributed data interference (FDDI) on the same twisted pair cable, simultaneously. These other WLAN users of the media are often uncoordinated with IEEE 802.11 and, in most cases, do not provide for any mechanism to share the media at all. Finally, there are other IEEE 802.11 WLANs sharing the media.

Since any one connect to a WLAN, it need to identify the stations connecting to the WLAN to identify the stations and protect the data.

Another challenge is mobilitiy. Dealing with mobility while making all of the expected LAN services available is a problem to be solved by MAC management.

And power management is the final challenge, conserving the energy stored in the batteries to allow the equipment to operate for as long as possible must be built into the WLAN protocol and controlled by MAC management.

3.1 Tools Available to Meet the Challenges

3.1.1 Authentication

Authentication provides a mechanism for one station to prove its identity to another station in the WLAN. Authentication can be used between any two stations. However, it is most useful when used between a mobile station and an AP in an infrastructure LAN. In this case, mobile station connect ESS and wired LAN behind

it through AP and full proof of the identity of the mobile station is necessary if the network is to be protected from unauthorized users.

There are two authentication algorithm. "Open system authentication" is a guaranteed result of success after two station introduce themselves to each other. No verification is needed.

The second authentication algorithm is the "shared key authentication algorithm". This algorithm depends on both stations having a copy of a shared WEP key. This algorithm uses the WEP encryption option to encrypt and decrypt a "challenge text" as the proof that the stations share the same key. Beginning the authentication process, station A sends its identity assertion to station B. Station B responds to the assertion with an assertion of its own and a request to station A to prove its identity by correctly encrypting the challenge text. Station A encrypts the challenge text using the normal WEP encryption rules, including use of default and key mapping keys, and sends the result back to station B. Station B decrypts the frame using the appropriate key and returns an authentication management frame to station A with the success of failure of the authentication indicated. If the authentication is successful, the standard says that each station is authenticated to the other.

A station may authenticate with any number of other stations. Always mobile performs the encryption operation on the challenge text and AP somehow occupied in a more privileged position. This leaves the IEEE 802.11 WLAN open to some not so subtle security problems. In particular, a rogue AP could adopt the SSID of the ESS and announce its presence through the normal beaconing process. A rogue could then simply complete normal frame handshake procedures and the mobile stations would be the victims of a denial of service attack. A more active rogue could use more subtle means to attempt to gain access to the content of higher layer protocol frames containing user names, passwords, and other sensitive data. If the data is encrypted using WEP, it is highly unlikely that the rogue could successfully decrypt the information.

3.1.2 Association

Association is the mechanism through which IEEE 802.11 provides transparent mobility to stations. Association may only be accomplished after a successful authentication has been completed.

When a mobile station requests to be connected to the WLAN, it sends an association request to an AP. The association request includes information on the capabilities of the station, such as the data rates it supports, the high rate PHY options it supports, its contention-free capabilities, its support of WEP, and any request for contention-free services. The association request also includes information about the length of time that the station may be in a low power operating mode. *The policies and algorithms used by the AP to make the decision of accepting the association request of the mobile station are not described in the standard.* Some things that may be considered are supporting all of the required data rates and PHY options, requiring contention-free services beyond the ability of the AP to support, long periods in low power operation that require excessive buffer commitments from the AP, and the number of stations currently associated. Because the standard does not specify what information may be considered by the AP when deciding to grant an association, information not local to the AP may also be used, such as load balancing factors and availability of other APs nearby. When the AP responds to the mobile station with an association response, the response includes a status indication. The status indication provides the mobile station with the success or failure of

the association request. If the request fails, the reason for that failure is in the status indication.

Once a station is associated, the AP is responsible for forwarding data frames from the mobile station toward their destination. If the destination is in the same BSS as the mobile station, AP will simply transmit the data frame to the BSS. If the destination of a data frame is outside the BSS, the AP will send the frame into the DS. If the destination is in another BSS, the AP sends the frame to the AP of the other BSS, where it will be forwarded to the mobile station. If the destination of the frame is entirely outside the ESS, the AP will forward the frame to the **portal**, the exit from the DS to the rest of the network. A **portal** is simply a transfer point between the wired LAN and the ESS, where frames logically enter the ESS. A **portal** may be an AP, a bridge, or a router. Because IEEE 802.11 is one of the family of IEEE 802 standards, an IEEE 802.11 frame must be translated from the IEEE 802.11 format to the format of the other LAN. This translation should be done according to IEEE Std 802.1h for bridging IEEE 802.11 to another LAN. The entire IEEE 802.11 frame, including MAC header and FCS, should not be encapsulated within another MAC protocol.

Similarly, when a data frame is sent from outside the ESS to a mobile station, the portal must forward the frame to the correct AP, the one that has the mobile station associated in its BSS.

Once a station is successfully associated, it may begin exchanging data frames with the AP. When the mobile loose contact with the AP, the mobile station must begin a new association in order to continue exchanging data frames. Because the DS must maintain information about the location of each mobile station and because data frames may have been sent to an AP with which the mobile station no longer can communicate, a mobile station will use a reassociation request after its initial association. The AP that has just granted the reassociation normally communicates with the AP with which the station was last associated to cause the termination of the old association.

3.1.3 Address Filtering

There may be more than one IEEE 802.11 WLAN operating in the same location and on the same medium and channel. In this case, the receiver must examine more than the destination address to make correct receive decisions. IEEE 802.11 incorporates at least three addresses in every data and management frame that may be received by a station. In addition to the destination address, these frames also include the BSS identifier. A station must use both the destination address and the BSSID when making receive decisions, according to the standard.

3.1.4 Privacy MAC Function

The privacy function is provided by the WEP mechanism. Described in Chapter 2.

3.1.5 Power Management

Power Management in an Independent BSS

In an independent BSS (IBSS), power management is a fully distributed process, managed by the individual mobile stations. Power management comprises two parts: the functions of the station entering a low power

operating mode and the functions of the stations that desire to communicate with that station. For a station to enter a low power operating state, a state where it has turned off the receiver and transmitter to conserve power, the station must successfully complete a data frame handshake with another station with the power management bit set in the frame header. The IEEE 802.11 standard does not specify when a station may enter or leave a low power operating state, only how the transition is to take place.

In the power saving state, the station must wake up to receive every Beacon transmission. The station must also stay awake for a period of time after each Beacon, called the announcement or ad hoc traffic indication message window (ATIM). The earliest the station may reenter the power saving state is at the conclusion of the ATIM window. The reason that a station must remain awake during the ATIM window is that other stations that are attempting to send frames to it will announce those frames during the ATIM window. If the power saving station receives an ATIM frame, it must acknowledge that frame and remain awake until the end of the next ATIM window, following the next Beacon frame, in order to allow the other station to send its data frame. *A station desiring to send a frame to another station in an IBSS, the standard requires that the sending station estimate the power saving state of the intended destination. How the sending station creates its estimate is not described in the standard.* If the station determines that the destination is in power saving state, then the station delays its transmission until it has received an acknowledgement of an ATIM frame.

Multicast frames must also be announced by the sending station during the ATIM window before they may be transmitted. The ATIM is sent to the same multicast address as the data frame that will be sent subsequently. Because the ATIM is sent to a multicast address, no acknowledgement will be generated, nor is one expected. Any stations that wish to receive the announced multicast data frame must stay awake until the end of the next ATIM window, after the next Beacon frame.

The power management mechanism puts a slightly greater burden on the sending station than on the receiving station. Sending stations must send an announcement frame in addition to the data frame it desires to deliver to the destination. Sending stations must buffer the frames to be sent to the power saving destination until the destination awakens and acknowledges the ATIM. Each transmission of an ATIM consumes power at the sending station. The receiving station must awaken for every Beacon and ATIM window, but need not make any transmissions unless it receives an ATIM frame.

Power Management in an Infrastructure BSS

In an infrastructure BSS, the power management mechanism is centralized in the AP. This power management mechanism allows much greater power savings for mobile stations than does the mechanism used in IBSSs. This is so because the AP assumes all of the burden of buffering data frames for power saving stations and delivering them when the stations request, allowing the mobile stations to remain in their power saving state for much longer periods.

Mobile station informs the AP, in its association request, of the number of beacon periods that the station will be in its power saving mode, to awaken at the expected time of a Beacon transmission to learn if there are any data frames waiting, and to complete a successful frame handshake with the AP, while the power management bit is set, to inform the AP when the station will enter the power saving mode.

A mobile station can achieve much deeper power savings than in the IBSS, because it is not required to awaken for every Beacon, nor to stay awake for any length of time after the Beacons for which it does awaken. The mobile station must also awaken at times determined by the AP, when multicast frames are to be delivered. This time is indicated in the Beacon frames as the delivery traffic indication map (DTIM).

The AP will buffer data and multicast frames if it has any stations associated that are in the power saving mode until a minimum time not less than the number of Beacon periods indicated in the mobile station‘s associated request. The standard indicates an aging algorithm to discard buffered frames that are older than it is required to preserve, though a specific algorithm is not described. AP indicate the frames buffered for a power saving station in the traffic indication map (TIM) sent with each Beacon frame. Each mobile station has an AID assigned in the association. When the bit in the TIM is set, there is at least one frame buffered for the corresponding station. When the bit is clear, there are no frames buffered for the corresponding station. A special AID is dedicated to indicate the status of buffered multicast traffic and the AP will send the TIM, with every beacon.

If an AP has any buffered multicast frames, those frames are sent immediately after the Beacon announcing the DTIM. If there is more than one multicast frame to be sent, the AP will indicate this fact by setting the more data bit in the frame control field of each multicast frame except for the last to be sent.

A mobile station requests delivery of buffered frames by sending a PS-Poll frame to the AP. The AP will respond to each PS-Poll with a frame where more data bit is set. Mobile station is required to send a PS-Poll to the AP for each data frame it receives with the more data bit set.

An AP that is also a PC running a contention-free period (CFP) will use the CFP to deliver buffered frames to stations that are CF Pollable. It may also use the CFP to deliver multicast frames after the DTIM is announced.

3.1.6 Synchronization

Synchronization is the process of the stations in a BSS getting in step with each other, so that reliable communication is possible. The MAC provides the synchronization mechanism to allow support of physical (PHY) layers that make use of frequency hopping or other time-based mechanisms where the parameters of the PHY layer change with time. The process involves beaconing, to announce the presence of a BSS, and scanning, to find a BSS. Once a BSS is found, a station joins the BSS. This process is entirely distributed, in both independent and infrastructure BSSs, and relies on a common timebase, provided by a timer synchronization function (TSF).

Timer Synchronization in an Infrastructure BSS

In an infrastructure BSS, the AP is responsible for transmitting a Beacon frame periodically. The beacon period is included as part of the information in the Beacon frame in order to inform stations receiving the Beacon when to expect the next Beacon. The Beacon may be delayed beyond the target Beacon transmission time due to other traffic occupying the medium and backoff delays. The beacon is not retransmitted in case of a collision since the becon frame is sent to broadcast address.

Synchronization function is very simple. A mobile station will update its TSF timer with the value of the timer it receives from the AP in the Beacon frame, modified by any processing time required to perform the update operation.

Timer Synchronization in an IBSS

In an IBSS, timer synchronization mechanism is completely distributed among the mobile stations of the BSS. The mobile station that starts the BSS will begin by resetting its TSF timer to zero and transmitting a Beacon, choosing a beacon period. Each station will attempt to send a Beacon after the TBTT arrives. The stations backoff for a random time to send the Beacon, In this random time, if a station hears a beacon it cancels its transmission. Corruption of beacon frames is allowed in the standard.

Beaconing also interacts with power management in the independent BSS. The standard requires that the station, or stations, that send a Beacon frame must not enter the power save state until they receive a Beacon frame from another station in the BSS. This restriction on the beaconing stationis to ensure that there is at least one station in the IBSS awake and able to respond to probe request frames.

The rules for updating the TSF timer is slightly more complex than those for stations in an infrastructure BSS. The station will update its TSF timer with the value of the received Beacon frame if the received value, after modifying it for processing times, is greater than the value currently in the timer. The effect of this selective updating of the TSF timer and the distributed nature of beaconing in an independent BSS is to spread the value of the TSF timer of the station with the fastest running clock throughout the BSS. If there is small number of stations, timers of the stations will be updated with the fastest timer value with a period proportional to the number of stations in the BSS. As the number of stations grows and collision of Beacon transmissions occurs, the spread of the fastest timer value will slow. Similarly if all stations cannot communicate directyly, it requires more than one station to propagate the fastest timer value to the outlying reaches of the BSS. Thus, the spread of the fastest timer value slows proportional to the number of hops it must take to reach all stations.

Synchronization with Frequency Hopping PHY Layers

Similar to beaconing, changes in a frequency hopping PHY layer (movements to other channels) occurs periodically (the dwell period). All stations in a BSS will change to the new channel when the TSF timer value, modulo the dwell period, is zero.

Scanning

In order for a mobile station to communicate with other mobile stations in an IBSS or with the AP in an infrastructure BSS, it must first find the stations or APs. The process of finding another station or AP is scanning. Scanning may be either passive or active.

- Passive scanning involves only listening for IEEE 802.11 traffic. It minimizes the power expended, while scanning the medium. The process a station uses is to move to a channel and listen for Beacon and

probe response frames, extracting a description of a BSS from each of these frames received. At the conclusion of the passive scan, the station accumulates information about the BSSs that are in the vicinity. Power is saved at the expense of more time consuming.

- Active scanning requires the scanning station to transmit and elicit responses form IEEE 802.11 stations and APs. It saves time spent scanning. The station does this by actively transmitting queries that elicit responses from stations in a BSS. The mobile move to a channel and transmits a probe request frame. If there is BSS on the channel that matches the SSID in the probe request frame, the station in that BSS that sent the latest Beacon frame will respond by sending a probe response frame to the scanning station. This is the AP in the infrastructure BSS and last station to send a Beacon in an IBSS.

Vendors are free to innovate and create their own policies regarding the use of active and passive scanning.

Joining a BSS

IEEE 802.11 standard does describe what is required of a station to join a BSS, it does not describe how a station should choose one BSS over another.

- It requires all of the mobile station‘s MAC and PHY parameters be synchronized with the desired BSS. Station updates its TSF timer with the value of the timer from the BSS description, modified by adding the time elapsed since the description was acquired. This will synchronize the TSF timer to the BSS.
- It will also coincidentally, synchronize the hopping of frequency hopping PHY layers.
- The station must also adopt the PHY parameters in the FH parameter set and /or the DS parameter set, as well as the required data rates to ensure that the PHY layer is operating on the same channel.
- The BSSID of the BSS must be adopted and the capability information field, such as WEP and the IEEE 802.11b high rate PHY capabilities.
- The beacon period and DTIM period must also be adopted.

Once this process is complete, the mobile station has joined the BSS and is ready to begin communicating with the stations in the BSS.

3.2 Combining Management Tools

3.2.1 Combine Power Saving Periods with Scanning

With this combination, a mobile station would complete the frame handshake with its AP to inform the AP that the station would be entering the power saving mode. The AP would then begin buffering any arriving data frames for the mobile station. Then, instead of entering the power saving mode, the mobile station

would perform active or passive scanning for a period of time, gathering BSS descriptions of other BSSs in the vicinity.

The combination allows a mobile station to gather information about its environment, the other BSSs that are nearby. When the mobile station eventually does move out of communication with its AP, it has all of the information available to it. This minimizes the disruption of communication when it is necessary for a mobile station to roam from one BSS to another.

3.2.2 Preauthentication

A mobile station combines scanning with authentication. As the mobile station scans for other BSSs, it will initiate an authentication when it finds a new BSS. This also reduces the time required for a station to resume communication with a new BSS, once it loses communication with the current BSS.

Some vendors choose to propagate an station‘s authentication from one AP to another through the DS, IEEE 802.11 standard does not discuss this,nor does it prohibit it.

Chapter 4

MAC Management Information Base

The IEEE 802.11 management information base (MIB) is an SMNPv2 managed object that contains a number of configuration parameters that allow an external management agent to determine the status and configuration of an IEEE 802.11 station.

The MAC MIB comprises two sections: the station management attributes and the MAC attributes. The station management attributes are associated with the configuration of options in the MAC and the operation of MAC management. The MAC attributes are associated with the operation of the MAC and its performance.

4.1 Station Management Attributes

dot11StationID is a 48 bit attribute that is designed to allow an external manager to assign its own identifier to a station. Default value is the unique MAC address of the station.

dot11MediumOccupancyLimit attribute provides a limit to the amount of time that the PC may control access to the medium. After this limit is reached, the PC must relinquish control of the medium to the DCF, allowing at least enough time to transmit a single maximum length MPDU, with fragmentation, before taking control of the medium again. The default value is 100 TU (1024 μs.)

dot11CFPPollable read-only unchangeable attribute is a Boolean flag that indicates the capability of the station to respond to the CF-Poll frame.

dot11CFPPeriod attribute defines the length of the CFP,in units of the DTIM interval, Duration is in units of DTIM and DTIM is in units of TU.

dot11CFPMaxDuration is equal to **dot11MediumOccupancyLimit**.

dot11AuthenticationResponseTimeout attribute places an upper limit, in TU, on the time a station is allowed before the next frame in an authentication sequence is determined not to be forthcoming.

dot11PrivacyOptionImplemented is a Boolean indicator of the presence of the privacy option.

dot11PowerManagementMode indicates the state of power management in the station.

dot11DesiredSSID indicates the SSID used during the latest scan operation by the station.

dot11DesiredBSSType indicates the type of BSS that the station sought during the latest scan operation.

dot11OperationRateSet is a list of data rates that may be used by the station to transmit in the BSS with which it is associated.

dot11BeaconPeriod controls the time that elapses between target beacon transmission times. Any change in this attribute will require that any current BSS be dissolved and a new BSS started with the new beacon period.

dot11DTIMPeriod controls the number of beacon periods that elapse between DTIMs. Any change will be ineffective until the new BSS.

dot11AssociationResponseTimeout attribute places an upper limit on the amount of time that a station will wait for a response to its association request.

dot11DisassociateReason indicates the reason code received in the most recently received disassociation frame. An external manager can track the location and reasons that stations are disassociated from the WLAN, in combination with **dot11DisassociateStation**. If a large number of stations are indicating authentication failures, deauthentications, or disassociations, this may be an indication that an AP is misbehaving or that an attack is in progress against the WLAN.

dot11AuthenticationAlgorithm is an entry in a table that holds an entry for each authentication algorithm supported by the station.

dot11WEPDefaultKeyValue is an attribute holding one of the WEP default keys. It is only write-only. The standard specifies that reading this attribute shall return a value of zero or null.

There is a table of attributes for the WEP key mapping keys. This table holds three accessible attributes:

dot11KeyMappingAddress holds the MAC address of a station with which there exists a key mapping relationship.

dot11KeyMappingWEPOn Boolean value and indicates whether the key mapping key is to be used when communicating with the station with the corresponding address.

dot11KeyMappingValue is the key to be used when key mapping is used to communicate with the station with the corresponding address.

dot11PrivacyInvoked is a Boolean attribute that indicates when WEP is to be used to product data frames.

dot11WEPDefaultKeyID identifies which of the four default keys are to be used when encrypting data frames with a default key.

dot11WEPKeyMappingLength indicates the number of entries that may be held in the key mapping table. The minimum value for this attribute is 10, indicating that the key mapping table must hold at least 10 entries.

dot11ExcludeUnencrypted is a Boolean attribute that controls whether a station will receive unencrypted data frames. When an unencrypted data frame is discarded, the value of **dot11WEPExcludedCount** is incremented. If the dot11WEPExcludedCount is increasing rapidly, it may be due to a station that is misconfigured, attempting to exchange frames without encryption.

In the same way,**dot11WEPICVErrorCount** attribute tracks the number of encrypted frames that have been received and decrypted, but for which the ICV indicates the decryption was not successful.

The station management portion of the MIB also includes three notification objects, corresponding to three occurrences that are usually exceptional. The **dot11Disassociate** object is activated when a station receives a disassociation frame. The **dot11Deauthenticate** object is activated when the station receives a deauthentication frame. The **dot11AuthenticateFail** object is activated when the station does not complete an authentication sequence successfully.

4.2 MAC Attributes

The MAC attributes tune the performance of the MAC protocol, monitor the performance of the MAC, identity the multicast addresses that the MAC will receive, and provide identification of the MAC implementation.

dot11MACAddress is the unique, individual address of the MAC. 48-bit manufacturer-assigned, globally administered MAC address.

dot11RTSThreshold controls the transmission of RTS control frames prior to data and management frames. The default value is 2347.

dot11ShortRetryLimit controls the number of times a frame that is shorter than the **dot11RTSThreshold** will be transmitted without receiving an acknowledgement before that frame is abandoned and a failure is indicated to higher layer protocols.

dot11LongRetryLimit controls the number of times a frame that is equal to or longer than the **dot11RTSThreshol** will be transmitted without receiving an acknowledgement before that frame is abandoned and a failure is indicated to higher layer protocols.

dot11FragmentationThreshold attribute defines the length of the largest frame that the PHY will accept. Frames larger than this threshold must be fragmented. The default value of this attribute is dependent on the PHY layer parameter a MPDUMaxLength. If the value of aMPDUMaxLength is greater than or equal to 2346, the default value is 2346, otherwise the default value is aMPDUMaxLength.

dot11MaxTransmitMSDULifetime controls the length of time that attempts to transmit an MSDU will continue after the initial transmission attempt. Since there may be fragmentation and retry limits apply to only a single frame of the fragment stream, this timer limits the amount of bandwidth that may be consumed.

dot11MaxReceiveLifetime controls the length of time that a partial fragment stream will be held pending reception of the remaining fragments necessary for complete reassembly of the MSDU.

dot11ManufacturerID is a variable length character string that identifies the manufacturer of the MAC.

dot11ProductID is a variable length character string that identifies the MAC.

dot11TransmittedFragmentCount [1] is a counter that tracks the number of successfully transmitted fragments.

dot11MulticastTransmittedFrameCount is a counter that tracks only transmitted multicast frames.

dot11FailedCount is a counter that tracks the number of frame transmissions that are abandoned because they have exceeded either the **dot11ShortRetryLimit** or **dot11LongRetryLimit**. This provide an indication of the "condition" of a BSS.

dot11RetryCount [2] [3] is a counter that tracks the number of frames that required at least one retransmission before being delivered successfully. **dot11MultipleRetryCount** is a counter that tracks the number of frames that required more than one retransmission to be delivered successfully.

dot11FrameDuplicateCount is a counter that tracks the number of duplicate frames received.

dot11RTSSuccessCount is a counter that increments for each CTS received in response to an RTS. **dot11RTSFailureCount** is a counter that increments each time a CTS is not received in response to an RTS.

dot11ACKFailureCount is a counter that tracks the number of times a data or management frame is sent to an individual address and does not result in the reception of an ACK frame from the destination.

dot11ReceivedFragmentCount is a counter that tracks the number of fragments received.

dot11MulticastReceivedCount is a counter that track the number of frames received by the station that match a multicast address in the group addresses table or were sent to the broadcast address.

---

[1] **dot11TransmittedFragementCount-dot11MulticastTransmittedFrameCount** indicates the number of individually addressed frames transmitted.

[2] **dot11RetryCount-dot11MultipleRetryCount** The number of frames delivered successfully after only one retransmission.

[3] **The number of individually addressed frames -dot11RetryCount** indicates the number of frames delivered successfully on the first transmission attempt.

dot11FCSErrorCount is a counter that tracks the number of frames received, of any type, that resulted in an FCS error. Increasing load and increasing error rate will both result in this counter increasing more rapidly.

dot11TransmittedFrameCount is a counter that tracks the number of MSDUs that have been transmitted successfully. This counter increments only if the entire fragment stream required to transmit an MSDU is sent and an acknowledgement is received for every fragment.

dot11WEPUndecryptableCount is a counter that tracks the number of frames received without FCS errors and with the WEP bit indicating that the frame is encrypted, but that can not be decrypted due to the **dot11WEPOn** indicating a key mapping key is not valid or the station not implementing WEP.

dot11Address attribute stores the multicast addresses. This attribute is one entry in the **dot11GroupAddressesTa**

dot11ResourceTypeIDName is an attribute required by IEEE 802.1F. It is a read-only, fixed-length character string. Its default value is "RTID".

dot11ResourceInfoTable contains four more attributes required by IEEE 802.1F

- **dot11manufacturerOUI** contains the IEEE-assigned 24-bit organizational unique identifier that forms half of a globally administered MAC address.
- **dot11manufacturerName** is a variable length character string containing the name of the manufacturer of the MAC.
- **dot11manufacturerProductName** is also a variable length character string containing the product identifying information for the MAC.
- **dot11manufacturerProductVersion** is also a variable length character string that identifies the version information for the MAC.

Chapter 5

The Physical Layer

5.1 Physical Layer (PHY) Functionality

The PHY is the interface between the MAC and wireless media, which transmits and receives data frames over a shared wireless media. The PHY provides three levels of functionality: First, the PHY layer provides a frame exchange between the MAC and PHY under the control of the physical layer convergence procedure (PLCP) sublayer. Secondly, the PHY uses signal carrier and spread spectrum modulation to transmit data frames over the media under the control of the physical medium dependent (PMD) sublayer. Thirdly, the PHY provides a carrier sense indication back to the MAC to verify activity on the media.

The standard is designed to meet the radio frequency (RF) emissions guidelines specified by the Federal Communications Commission (FCC), European Telecommunications Standard Institute (ETSI), and Ministry of Telecommunications (MKK).

5.2 Direct Sequence Spread Spectrum (DSSS) PHY

The DSSS uses the 2.4 GHz frequency band as the RF transmission media. Data transmission over the media is controlled by the DSSS PMD sublayer as directed by the DSSS PLCP sublayer.

The DSSS PMD takes the binary bits of information from the PLCP protocol data unit (PPDU) and transforms them into RF signals for the wireless media by using carrier modulation and DSSS techniques. Figure 5.2 illustrates the basic of elements of the DSSS PMD transmitter and receiver.

5.2.1 DSSS PLCP Sublayer

The PLCP protocol data unit (PPDU) is unique to the DSSS PHY layer. The PPDU frame (See Figure 5.3) consists of a PLCP preamble, PLCP header, and MAC protocol data unit (MPDU). The PLCP preamble and PLCP header are always transmitted at 1 Mbps, and the MPDU can be sent at 1 Mbps or 2 Mbps.

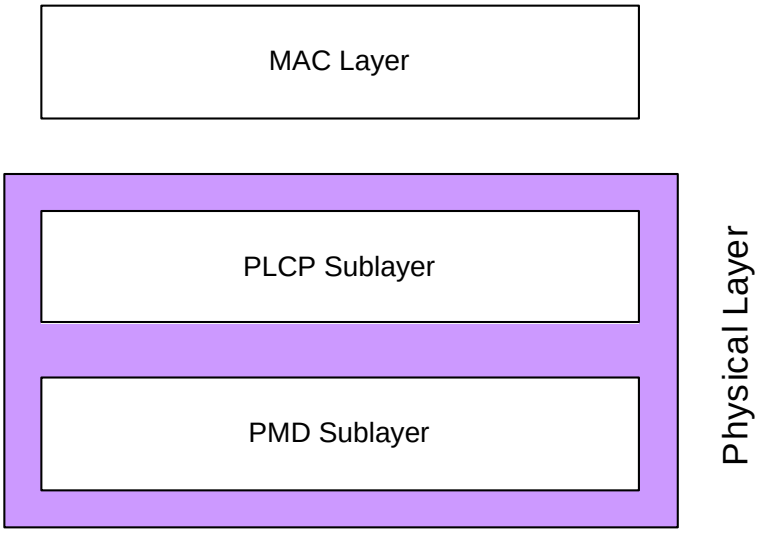


Figure 5.1: The OSI Model

SYNC This field is 128 bits in length and contains a string of 1s which are scrambled prior to transmission. The receiver uses this field to acquire the incoming signal and synchronize the receiver‘s carrier tracking and timing prior to receiving the start of frame delimiter (SFD).

Start of frame delimiter (SFD) This field contains information marking the start of a PPDU frame. The SFP specified is common for all IEEE 802.11 DSSS radios and uses the following hexadecimal word: F3A0hex.

Signal The signal field defines which type of modulation must be used to receive the incoming MPDU. The binary value in this field is equal to the data rate multiplied by 100 kbit/s. In the June 1997 version of IEEE 802.11, two rates are supported. They are: 0Ah for 1Mbps DBPSK and 14hex for 2 Mbps DQPSK.

Service The service field is reserved for future use and the default value is 00h.

Length The length field is an unsigned 16-bit integer that indicates the number of microseconds necessary to transmit the MPDU. The MAC layer uses this field to determine the end of a PPDU frame.

CRC The CRC field contains the results of a calculated frame check sequence from the sending station. The CRC-16 algorithm is represented by the following polynomial: $G(x) = x^{16} + x^{12} + x^5 + x^1$. The receiver performs the calculation on the incoming signal, service, and length fields and compares the results against the transmitted value. If an error is detected, the receiver‘s MAC makes the decision if incoming PPDU should be terminated.

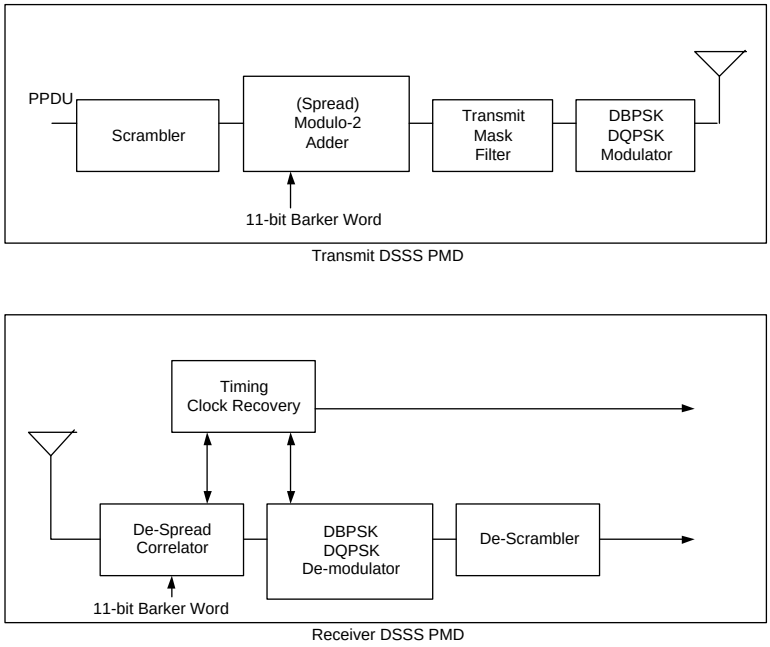


Figure 5.2: Transmit and Receive DSSS PMD

FCS field of the MPDU portion of the PPDU protects the information in the PLCP service data unit (PSDU). The DSSS PHY does not determine if errors are present in the MPDU. The MAC makes that determiation similar to the method used by the PHY layer.

5.2.2 Data Scrambling

All information bits transmitted by the DSSS PMD are scrambled using a self-synchronizing 7-bit polynomial. The scrambling polynomial for the DSSS PHY is: $G(z) = z^{-7} + z^{-4} + 1$. Scrambling is used to randomize the data in the SYNC field of the PLCP and data patterns which contain long strings of binary 1s or 0s. The

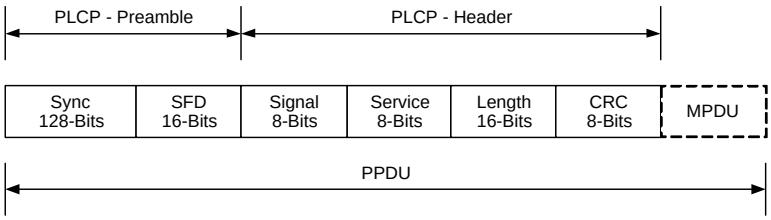


Figure 5.3: DSSS PHY PLCP Preamble, Header, and MPDU

receiver can descramble the information bits without prior knowledge from the sending station.

5.2.3 DSSS Modulation

The DSSS PMD transmits the PLCP preamble and PLCP header 1 Mbps using differential binary phase shift keying (DBPSK). The MPDU is sent at either 1 Mbps DBPSK or 2 Mbps differential quadrature phase shift keying (DQPSK), depending upon the content in the signal field of the PLCP header.

DPSK is noncoherent; a clock reference is not needed to recover the data. DQPSK is more tolerant to intersymbol interference caused by noise and multipath over the media; therefore DBPSK is used for the PLCP preamble.

5.2.4 Barker Spreading Method

The DSSS PHY layer is one of the two 2.4 GHz RF PHY layers to choose from in the IEEE 802.11 standard. In the transmitter

$$Barker\,word(11-bits)+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1$$

In the transmitter, the 11-bit Barker word is applied to a modulo-2 adder (Ex-Or function) together with each of the information bits in the PPDU. The PPDU is clocked at the information rate, 1 Mbps for example, and the 11-Barker word at 11 Mbps (the chipping block). The output of the modulo-2 adder results in a signal with a data rate that is 10x higher than the information rate. At the receiver, the DSSS signal is convolved with the 11-bit Barker word and correlated. The correlation operation recovers the PPDU information bits at the transmitted information rate, and the undesired interfering in-band signals are spread out-of-band. The spreading and despreading of narrowband to a wideband signal is commonly referred to as processing gain and measured in decibels (dB). Processing gain is the ratio of the DSSS signal rate to the PPDU information rate. The FCC and MKK specify the minimum requirement for processing gain in North America and Japan as 10 dB.

5.2.5 DSSS Operating Channels and Transmit Power Requirements

Each DSSS PHY channel occupies 22 MHz of bandwidth, and the spectral shape of the channel represents a filtered SinX/X function. The DS channel transmit mask in IEEE 802.11 specifies that spectral products be filtered to -30dBr from the center frequency and all other products be filtered to -50dBr. This allows for three noninterfering channels spaced 25 MHz apart in the 2.4 GHz frequency band. (See Figure 5.4)

In addition to frequency and bandwidth allocations, transmit power is a key parameter that is regulated worldwide. The maximum allowable radiated emissions for the DSSS PHY varies from region to region. Today in market wireless products have selected 100 mW as the nominal RF transmit power level.

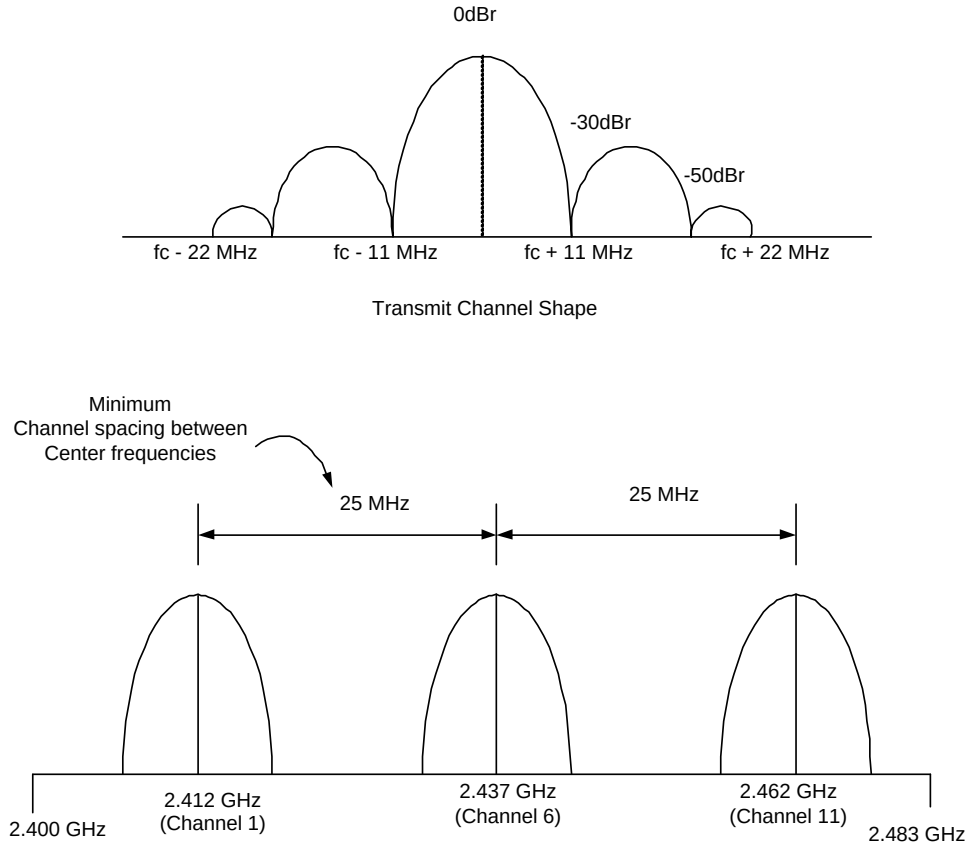


Figure 5.4: Channel Shape and Channel Spacing

5.3 The Frequency Hopping Spread Spectrum (FHSS) PHY

Data transmission over the media is controlled by the FHSS PMD sublayer as directed by the FHSS PLCP sublayer. The FHSS PMD takes the binary bits of information from the whitened PSDU and transforms them into RF signals for the wireless media by using carrier modulation and FHSS techniques. Figure 5.5 illustrates the basic elements of the FHSS PMD transmitter and receiver.

5.3.1 FHSS PLCP Sublayer

The PLCP preamble is used to acquire the incoming signal and synchronize the receiver‘s demodulator.

SYNC This field contains a string of alternating 0s and 1s patterns and is used by the receiver to synchronize

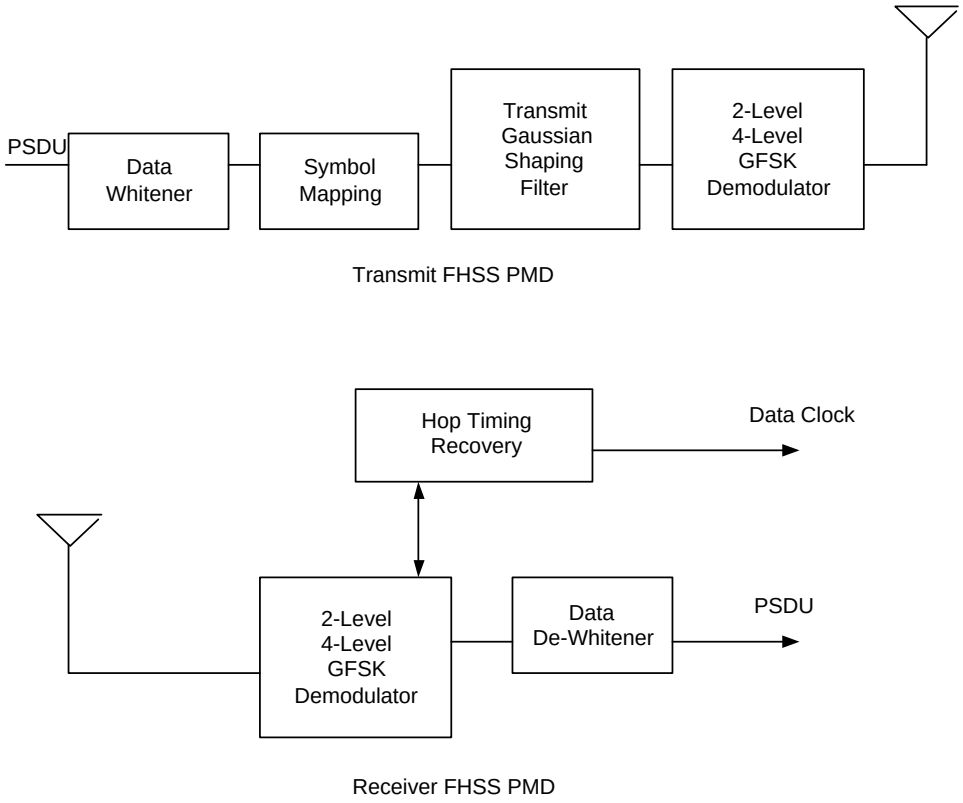


Figure 5.5: Transmit and Receive FHSS PMD

the receiver's packet timing and correct for frequency offsets.

SFD This field contains information marking the start of a PSDU. A common SFD is specified for all IEEE 802.11 FHSS radios using the following bit pattern: 0000110010111101.

PLW This field specifies the length of the PSDU in octets and is used by the MAC to detect the end of a PPDU frame.

PLCP signaling field (PSF): The PSF identifies the data rate of the whitened PSDU ranging from 1 Mbps to 4.5 Mbps in increments of 0.5 Mbps. The PLCP preamble and header are transmitted at the basic rate, 1 Mbps. The optional data rate for the whitened PSDU is 2 Mbps.

Header Check Error This field contains the results of a calculated frame check sequence from the sending station. The calculation is performed prior to data whitening. The CCIT CRC-16 error detection algorithm is used to protect the PSF and PLW fields.

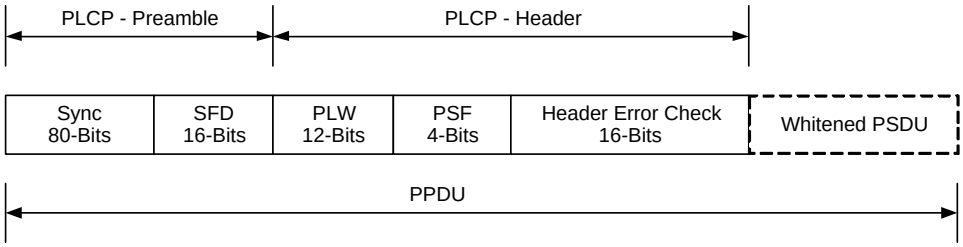


Figure 5.6: FHSS PHY PLCP Preamble, Header, and PSDU

The MAC makes the determination of the correct reception of PPDU frame by looking FCS which is embedded at the end of the PSDU portion of the PPDU.

5.3.2 PSDU Data Whitening

Data whitening is applied to the PSDU before transmission to minimize DC bias on the data if long strings of 1s or 0s are contained in the PSDU. The PHY stuffs a special symbol every 4 octets of the PSDU in a PPDU frame. A 127-bit sequence generator using the polynomial $S(x) = x^7 + x^4 + 1$ and 32/33 bias-suppression encoding algorithm are used to randomize and whiten the data.

5.3.3 FHSS Modulation

1997 version of IEEE 802.11 uses two-level Gaussian frequency shift key (GFSK) in the FHSS PMD to transmit the PSDU at the basic rate of 1 Mbps. The PLCP preamble and PLCP header are always transmitted at 1 Mbps. However, four-level GFSK is an optional modulation method defined in the standard that enables the whitened PSDU to be transmitted at a higher rate. The value contained in the PSF field of the PLCP header is used to determine the data rate of the PSDU.

GFSK is a modulation technique used by the FHSS PMD, which deviates (shifts) the frequency either side of the carrier hop frequency depending on if the binary symbol from the PSDU is either a 1 or 0. A bandwidth bit period (Bt) = 0.5 is used. The changes in the frequency represents symbols containing PSDU information. For two-level GFSK, a binary 1 represents the upper deviation frequency from the hopped carrier, and a binary 0 represents the lower deviation frequency. The deviation frequency (f_d) shall be greater than 110 KHz for IEEE 802.11 FHSS radios. The carrier frequency deviation is given by:

$$\begin{array}{c} \text{Binary } 1 = F_c + f_d \\ \text{Binary } 0 = F_c - f_d \end{array}$$

Four-level GFSK is similar to two-level GFSK and used to achieve a data rate of 2 Mbps in the same occupied frequency bandwidth. The modulator combines two binary bits from the whitened PSDU and encodes them into symbol pairs (10, 11, 01, 00). The symbol pairs generate four frequency deviations from the hopped carrier frequency, two upper and two lower. The symbol pairs are transmitted at 1 Mbps, and for each bit sent, the resulting data rate is 2 Mbps.

5.3.4 FHSS Channel Hopping

A set of hop sequences is defined in IEEE 802.11 for use in the 2.4 GHz frequency band. The channels are evenly spaced across the band over a span 83.5 MHz. Hop channels differs from country to country.

Channel hopping is controlled by the FHSS PMD. The FHSS PMD transmits the whitened PSDU by hopping from channel to channel in a pseudorandom fashion using one of the hopping sequences.

5.4 Infrared (IR) PHY

The IR PHY is one of the three PHY layers supported in the standard. The IR PHY differs from DSSS and FHSS because IR uses near-visible light as the transmission media. IR communication relies on light energy, which is reflected off objects or by line-of-sight. The IR PHY operation is restricted to indoor environments and cannot pass through walls, such as DSSS and FHSS radio signals. Data transmission over the media is controlled by the IR PMD sublayer as directed by the IR PLCP sublayer. See (Figure 5.7)

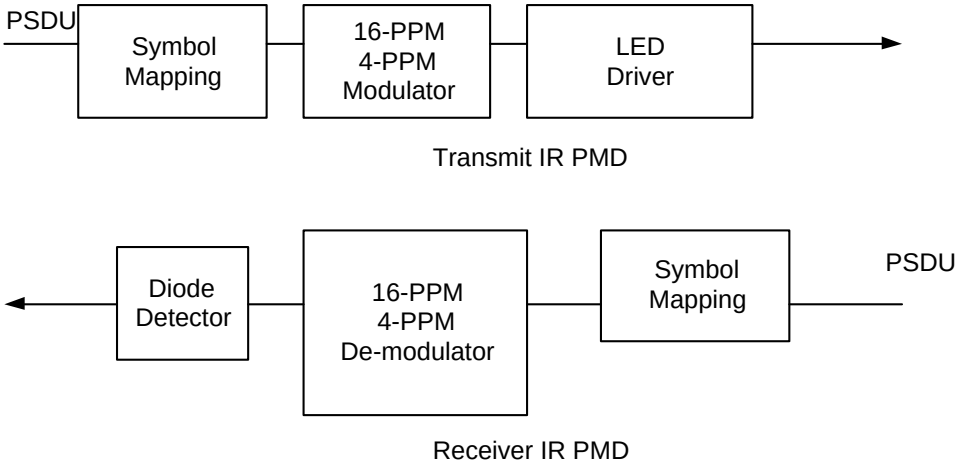


Figure 5.7: Transmit and Receive IR PMD

5.4.1 IR PLCP Sublayer

The PLCP preamble, PLCP header, and PSDU make up the PPDU, as shown in Figure 5.8. The PLCP preamble and PLCP header are unique to the IR PHY. The PLCP preamble is used to acquire the incoming signal and synchronize the receiver prior to the arrival of the PSDU. The PLCP header contains information about PSDU from the sending IR PHY. The PLCP preamble and PLCP header are always transmitted at 1 Mbps and the PSDU can be sent at 1 Mbps or 2 Mbps.

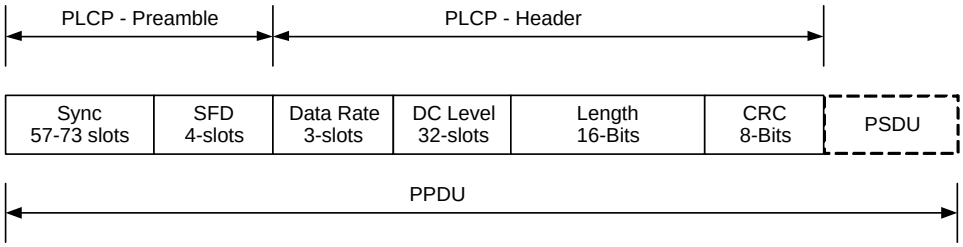


Figure 5.8: IR PHY PLCP Preamble, Header, and PSDU

SYNC This field contains a sequence of alternated presence and absence of a pulse in consecutive time slots. The SYNC field is used by the IR PHY to perform signal acquisition and clock recovery. The standard specifies 57 time slots as the minimum and 73 time slots as the maximum.

SFD This field contains information that marks the start of a PPDU frame. A common SFD is specified for all IEEE 802.11 IR implementations. The SFD is represented by the following bit pattern: 1001

Data Rate This field defines the data rate the PPDU is transmitted. There are two rates to choose from 000 for 1 Mbps (the basic rate) and 001 for 2 Mbps (the enhanced access rate). The PLCP preamble and PLCP header are always sent at the basic rate 1 Mbps.

DC level This field contains information that allows the IR PHY to stabilize the DC level after receiving the preamble and data rate fields.

Length This field contains an unsigned 16-bit integer that indicates the number of microseconds to transmit the PSDU. The MAC layer uses this field to detect the end of a frame.

Frame Check Sequence This field contains the calculated 16-bit CRC result from the sending station. The CCITT CRC-16 error detection algorithm is used to protect the length field. The receiver performs the calculation on the incoming Length field and compares the results against the transmitted field. If an error is detected, the receiver‘s MAC determines if the incoming PSDU should be terminated.

Again MAC uses the FCS to make the determination for PSDU.

5.4.2 IR PHY Modulation Method

The IR PHY transmits binary data at 1 and 2 Mbps using a modulation known as pulse position modulation (PPM). PPM is used IR systems to reduce the optical power required of the LED infrared source. The specific data rate is dependent upon the type of PPM. The modulation for 1 Mbps operation is 16-PPM and 4-PPM for 2 Mbps. PPM is a modulation technique that keeps the amplitude, pulse width constant, and varies the position of the pulse in time. Each position represents a different symbol in time.

For 2 Mbps operation 4-PPM is used and two data bits are paired in the PSDU to form a 4-bit symbol map as shown in Table 6.1.

Data Bits	4-PPM Symbol
00	0001
01	0010
11	0100
10	1000

Table 5.1: 4-PPM Symbol Map for 2 Mbps

5.5 Geographic Regulatory Bodies

WLAN IEEE 802.11-compliant DSSS and FHSS radios operating in the 2.4 GHz frequency band must comply with the local geographical regulatory domains before operating in this spectrum. The regulatory agencies in these regions set emission requirements for WLANs to minimize the amount of interference a radio can generate or receive from another in the same proximity.

Chapter 6

Physical Layer Extensions to IEEE 802.11

In October 1997 the IEEE 802 Executive Committee approved two projects to for higher rate physical layer (PHY) extensions to IEEE 802.11. The first extension, IEEE 802.11a, defines requirements for a PHY operating in the 5.0 GHz U-NII frequency and data rates ranging from 6 Mbps to 54 Mbps.

The second extension, IEEE 802.11b, defines a set of PHY specifications operating in the 2.4 GHz ISM frequency band up to 11 Mbps. Both PHY are defined to operate with the existing MAC.

6.1 IEEE 802.11a - The OFDM Physical Layer

The IEEE 802.11a PHY i adopts orthogonal frequency division multiplexing (OFDM) PHY. The OFDM PHY provides the capability to transmit PSDU frames at multiple data rates up to 54 Mbps for WLAN networks where transmission of multimedia content is a consideration.

6.1.1 OFDM PLCP Sublayer

The PPDU is unique to the OFDM PHY. The PPDU frame consists of a PLCP preamble and signal and data fields as shown in Figure 6.1.

The receiver uses the PLCP preamble to acquire the incoming OFDM signal and synchronize the demodulator. The PLCP header contains information about the PSDU from the sending OFDM PHY. The PLCP preamble and the signal field are always transmitted at 6 Mbps, binary phase shift keying (BPSK) - OFDM modulated using convolutional encoding rate R=1/2.

PLCP preamble This field is used to acquire the incoming signal and train and synchronize the receiver. The PLCP preamble consists of 12 symbols, ten of which are short symbols, and two long symbols. The short symbols are used to train the receiver‘s AGC and obtain a coarse estimate of the carrier frequency and the channel. The long symbols are used to fine-tune the frequency and channel estimates. Twelve sub-carriers are used for the short symbols and 53 for the long. The training of an OFDM is accomplished in 16 μs. PLCP preamble is BPSK-OFDM modulated at 6 Mbps.

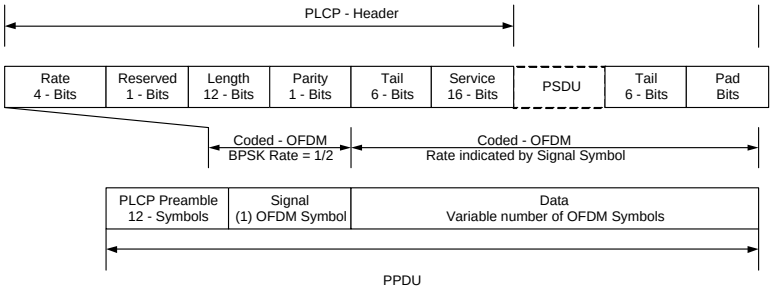


Figure 6.1: OFDM PLCP Preamble, Header, and PSDU

Rate	Modulation	Coding Rate	Signal bits (R1-R4)
6 Mbps	BPSK	R=1/2	1101
9 Mbps	BPSK	R=3/4	1111
12 Mbps	QPSK	R=1/2	0101
18 Mbps	QPSK	R=3/4	0111
24 Mbps	16QAM	R=1/2	1001
36 Mbps (opt.)	16QAM	R=3/4	1011
48 Mbps (opt.)	64QAM	R=2/3	0001
54 Mbps (opt.)	64QAM	R=3/4	0011

Table 6.1: PSDU Date Rate Selection

Signal The signal is a 24-bit field, which contains information about the rate and length of the PSDU. The Signal field is convolutional encoded rate 1/2, BPSK-OFDM modulated. Four bits (R1 - R4) are used to encode the rate, eleven bits are defined for the length, one reserved bit, a parity bit, and six "0" tail bits. the rate bits (R1-R4) are defined in Table 6.1. The mandatory data rates for IEEE 802.11a-compliant systems are 6 Mbps, 12 Mbps, and 24 Mbps.

Length The length field is an unsigned 12-bit integer that indicates the number of octets in the PSDU.

Data The data field contains the service field, PSDU, tails bits, and pad bits. A total of six tail bits containing 0s are appended to the PPDU to ensure that the convolutional encoder is brought back to zero state.

6.1.2 Data Scrambler

All the bits transmitted by the OFDM PMD in the data portion are scrambled using a frame-synchronous 127-bit sequence generator. Scrambling is used to randomize the service, PSDU, pad bit, and data patterns,

which may contain long strings of binary 1s or 0s. The tail bits are not scrambled. The scrambling polynomial for the OFDM PHY is: $S(x) = x^{-7} + x^{-4} + 1$.

6.1.3 Convolutional Encoding

All information contained in the service, PSDU, tail, and pad are encoded using convolutional encoding rate R=1/2, 2/3, 3/4 corresponding to the desired data rate.

6.1.4 OFDM Modulation

OFDM method chosen for IEEE 802.11a is similar to the modulation technique adopted in Europe by ETSI-HIPERLAN II 5 GHz radio PHY specification.

The basic principal of operation first divides a high-speed binary signal to be transmitted into a number of lower data rate subcarriers. There are 48 data subcarriers and 4 carrier pilot subcarriers for a total of 52 nonzero subcarriers defined in IEEE 802.11a. Each lower data rate bit stream is used to modulate a separate subcarrier from one of the channels in the 5 GHz band.

Intersymbol interference is generally not a concern for lower speed carrier, however the subchannels may be subjected to frequency selective fading. Therefore, bit interleaving and convolutional encoding is used to improve the bit error rate performance.

The scheme uses integer multiples of the first subcarrier, which are orthogonal to each other. This technique is known as orthogonal frequency division multiplexing (OFDM).

Prior to transmission the PPDU is encoded using a convolutional coded rate R=1/2, and the bits are reordered and bit interleaved for the desired data rate. Each bit is then mapped into a complex number according the modulation type and subdivided in 48 data subcarriers and 4 pilot subcarriers. The subcarriers are combined using an inverse fast fourier transform and transmitted. At the receiver, the carrier is converted back to a multicarrier lower data rate form using an FFT. The lower data subcarriers are combined to form the high rate PPDU. An example of an IEEE 802.11a OFDM PMD is illustrated in Figure 6.2.

6.1.5 OFDM Operating Channels and Transmit Power Requirements

The 5 GHz U-NII frequency band is segmented into three 100 MHz bands for operation in the US. The lower band ranges from 5.15-5.25 GHz, the middle band ranges from 5.25-5.35 GHz and the upper band ranges from 5.725-5.825 GHz. The channel frequencies and numbering defined in IEEE 802.11a start at 5 GHz. Three transmit RF power levels are specified; 40 mW, 200 mW and 800 mW.

6.1.6 Geographic Regulatory Bodies

WLAN IEEE 802.11a-compliant OFDM radios operating in the 5 GHz UNII frequency band must comply with the local geographical regulatory domains before operating in this spectrum.

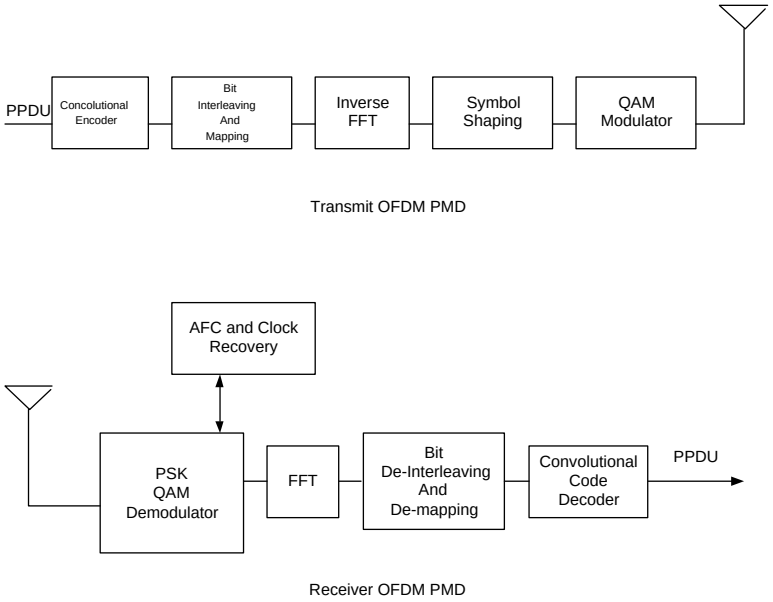


Figure 6.2: IEEE 802.11a Transmit and Receive OFDM PMD

6.2 IEEE 802.11b-2.4 High Rate DSSS PHY

The IEEE 802.11b PHY is one of the PHY layer extensions of IEEE 802.11 and is referred to as high rate direct sequence spread spectrum (HR/DSSS). HR/DSSS PHY provides two functions. First, the HR/DSSS extends the PSDU data rates to 5.5 Mbps and 11 Mbps using an enhanced modulation technique. Secondly, the HR/DSSS PHY provides a rate shift mechanism, which allows 11 Mbps networks to fall back to 1 and 2 Mbps and interoperate with the legacy IEEE 802.11 2.4 GHz RF PHY layers. The OSI structure and operation of the PHY‘s PLCP sublayer and PMD sublayer for HR/DSSS is similar to the existing IEEE 802.11 DSSS PHY described in Chapter 5.

6.2.1 HR/DSSS PHY PLCP Sublayer

The HR/DSSS PHY defines two PLCP preambles, long and short (see Figure **??**. The long preamble uses the same PLCP preamble and header as the IEEE 802.11 DSSS PHY and sends the information at 1 Mbps using DBPSK and Barker word direct sequence spreading. The PSDU is transmitted at 1,2,5.5, and 11 Mbps as determined by the content in the signal field. The long preamble is backwards compatible with existing IEEE 802.11 DSSS PHY and defined to interoperate with existing IEEE 802.11 wireless networks operating at 1 and 2 Mbps.

SYNC The receiver uses this field to acquire the incoming signal and synchronize the receiver‘s carrier tracking and timing prior to receiving the SFD.

SFD This field contains information marking the start of a PPDU frame. The SFD specified is common for all IEEE 802.11 DSSS and IEEE 802.11b long preamble radios.

Signal The signal field defines which type of modulation must be used to receive the incoming PSDU. The binary value in this field is equal to the data rate multiplied by 100 kbit/s.

Service The service field uses 3 bits of the reserved 8 bits for IEEE 802.11b. Data bit (b2) determines whether the transmit frequency and symbol clocks use the same local oscillator. Data bit (b3) indicates whether complimentary code keying (CCK) or packet binary convolutional coding (PBCC) is used and data bit (b7) is a bit extension used in conjunction with the length field to calculate the duration of the PSDU in micoseconds. This field is used for the long and short preamble frames.

Length The length field is an unsigned 16-bit integer that indicates the number of microseconds necessary to transmit the PSDU.

CRC The CRC field contains the results of a calculated frame check sequence from the sending station. The calculation is performed prior to data scrambling for the long and short preamble. The CCITT CRC - 16 error detection algorithm is used to protect the signal,service and length fields.

6.2.2 High Rate Data Scrambling

All information bits transmitted by the DSSS PMD are scrambled using a self-synchronizing 7-bit polynomial. The scrambling polynomial for the DSSS PHY is : $G(z) = z^{-7} + z^{-4} + 1$.

6.2.3 IEEE 802.11 High Rate Operating Channels

The HR/DSSS PHY uses the same frequency channels as defined in Chapter 5 for the IEEE 802.111 direct sequence PHY.

6.2.4 IEEE 802.11 DSSS High Rate Modulation and Data Rates

There are four modulation formats and data rates defined in IEEE 802.11b. The data rates include the basic rate, the extended rate, and enhanced rate. The basic rate is defined, as 1 Mbps modulated with DBPSK, and the extended rate is 2 Mbps DQPSK modulated. The 11-bit Barker word is used as the spreading format for the basic and extended rate as described for the DSSS PHY in Chapter 5. The enhanced rate is defined to operate at 5.5 Mbps and 11 Mbps using CCK modulation and packet binary convolutional coding (PBCC). PBCC is an option in the standard for those networks requiring enhanced performance. Frequency agility is another option defined in IEEE 802.11b. As with the 1 and 2 Mbps DSSS PHY, this option enables existing IEEE 802.11 FHSS 1 Mbps networks to be interoperable with 11 Mbps CCK high rate networks.

6.2.5 Complementary Code Keying (CCK) Modulation

CCK for the high rate extension to deliver PSDU frames at speeds of 5.5 Mbps and 11 Mbps was adopted because it easily provides a path for interoperability with existing IEEE 802.11 1 and 2 Mbps systems by maintaining the same bandwidth and incorporating the existing DSSS PHY PLCP preamble and header.

6.2.6 DSSS Packet Binary Convolutional Coding

Packet binary convolutional coding (PBCC) is an optional coding scheme defined in IEEE 802.11b. The coding option uses a 64-state binary convolutional code (BCC), rate R=1/2 code, and a cover sequence. The HR/DSSS PMD uses PBCC to transmit the PPDU. To ensure that the PPDU frame is properly decoded at the receiver, the BCC encoder‘s memory is cleared at the end of a frame.

6.2.7 Frequency Hopped Spread Spectrum (FHSS)Inter operability

A channel agility option is defined in IEEE 802.11b which allows IEEE 802.11 FHSS 1 and 2 Mbps networks to interoperate with HR/DSSS 11 Mbps WLANs. Both nonoverlapping and overlapping high rate channels are supported. The nonoverlapping allows WLAN systems to operate simultaneously in the same area without interfering with each other. Two sets of hopping sequence are defined for worldwide operation. For more details on the hop patterns refer to IEEE 802.11b.

Chapter 7

System Design Considerations for IEEE 802.11 WLANs

The IEEE 802.11 WLAN standard provides a number of physical layer options in terms of data rates, modulation types, and spreading spectrum techniques. Selecting the right physical layer and MAC technologies requires careful planning and detailed systems analysis for developing the optimal WLAN implementation.

7.1 The Medium

The difference between "wired" and RF WLANs is the radio communications link. While the radio communications link provides the freedom to move without constraints of wires, the wired media has the luxury of a controlled propagation media. Wireless RF medias are very difficult to control because the dynamics of the propagated signals over the media are constantly changing. RF medium is understood to properly design 2.4 GHz and 5 GHz IEEE 802.11 WLAN systems, especially for networks operating at data rates greater than 2 Mbps since these bands are shared with unlicenced users.

7.2 Multipath

Multipath is one of the performance concerns for indoor IEEE 802.11 WLAN systems. Multipath occurs when the direct path of the transmitted signal is combined with paths of the reflected signal paths, resulting in a corrupted signal at the receiver. The delay of the reflected signals known as delay spread is measured in nanoseconds. Delay spread is the parameter used to signify multipath. The amount of delay spread varies for environments see Table **??**.

RAKE processing and equalization are two methods used to process and resolve delay spread. A RAKE receiver is well-known architecture used to remove delay spreads on the order of 100nsec. The RAKE is structured as a bank of correlators (fingers) with weighed delays and a combiner. Equalization is an alternative

Environment	Delay Spread
Home	¡50 nsec
Office	˜100 nsec
Manufacturing floor	200-300 nsec

used to correct delay spreads greater than 100 nsec. Multipath causes the signals from the previous symbol to interfere with the signals of the next.

7.3 Multipath Channel Model

The IEEE 802.11 Working Group adopted the following channel model as the baseline for predicting multipath for modulations used in IEEE 802.11a (5 GHz) and IEEE 802.11b (2.4 GHz). This model is ideal for software simulations predicting performance results of a given implementation.

The channel response is composed of complex samples with random uniformly distributed phase and Rayleigh distributed magnitude with average power decaying exponentially. The mathematical model is as follows.

$$h_k = N(0, \frac{1}{2}\sigma_k^2) + jN(0, \frac{1}{2}\sigma_k^2)$$

$$\sigma_k^2 = \sigma_0^2 e^{-kT_s/T_{RMS}}$$

$$\sigma_0^2 = 1 - e^{-T_s/T_{RMS}}$$

Where $N(0, \frac{1}{2}\sigma_k^2)$ is a zero mean Gaussian random variable with variance $\frac{1}{2}\sigma_k^2$.

Let T_s be the sampling period and T_{RMS} be the delay spread of the channel. The performance assessment shall be no longer than the smaller of 1/(signal bandwidth) or $T_{RMS}/2$. The number of samples to be taken in the impulse response should ensure sufficient delay of the impulse response tail, e.g. $k_{max} = 10xT_{RMS}/T_s$.

7.4 Path Loss in a WLAN System

Another key consideration is the issue of operating range relative to path loss. This plays an important role in determining the size of overlapping WLAN cells and distribution of APs. Path loss calculations are equally important for determining the radio‘s receiver sensitivity and transmitting power level and signal to noise ratio (SNR) requirements.

For indoor applications beyond 20 feet, propagation losses increase at about 30 dB per 100 feet. This occurs because of a combination of attenuation by walls, ceilings, and furniture. Each wall constructed with

sheet rock and wood typically attenuates the signal by 6 dB and walls constructed with cement block walls attenuate the signal by 4 dB. However, additional losses may occur depending on the fading characteristics of the operating environment. The sam path principles apply for all frequency bands. However, as the operating frequency increases from 2.4 GHz to 5 GHz, for example, and additional path loss of 5-10 dB occurs. This results in a smaller cell radius and may require additional overlapping cells and APs to guarantee the same area as a system operating at 2.4 GHz.

7.5 Multipath Fading

Another key consideration is the path loss due to multipath fading. Multipath fading occurs when the reflected signal paths refract off people, furniture, windows, and scatter the transmitted signal. For example, moving the receiver from the transmitter a small distance even only a few inches, can produce an additional loss of signal power on the order of 20 dB or more. Multipath fading is viewed as two separate factors and described as probability distribution functions. The first factor is a characteristic known as log normal fading. These are coefficient products which result as the signal reflects off surfaces and propagates to the receiver. As the signal coefficients product propagate to the receiver, they are summed together with the direct path where they cancel each other, causing significant attention of the transmitted singal. This is the second factor, known as Rayleigh fading. RAKE architectures and equalization are techniques used to correct for these effects.

7.6 Es/No vs BER Performance

System performance tradeoffs are often made in the decision process when selecting a modulation type and data rate. System tradeoffs in terms of receiver sensitivity, range, and transmit power become very important for developing low cost implementations, especially for higher rate 2.4 GHz IEEE 802.11b systems.

7.7 Data Rage vs Aggregate Throughput

The IEEE 802.11 standard defines data rate in terms of symbol rate, or available bit rate. The PPDU data is modulated and transmitted over the RF or IR medium at this rate. This rate is often confused with the aggregate data throughput. The aggregate data rate, takes into account the overhead associated with protocol frame structure, collisions, and implementation processing delays associated with frames processed by mobile stations and APs. A good rule of thumb for estimating the average aggregate throughput of an IEEE 802.11 wireless network is 75% of the data rate for DCF operation, and 85% of the data rate for PCF.

7.8 WLAN Installation and Site Survey

A site survey is used to determine the maximum operating range between and AP (fixed location) and mobile stations for a specified transmit RF power level. Second, the survey helps identify holes of coverage due

to multipath, interference sources, and neighboring existing WLAN installations. Lastly, it is used in cell planning of overlapping BSAs and for layout of APs giving them hardwired access to existing wired Ethernet LAN infrastructures.

7.9 Interference in the 2.4 GHz Frequency Band

The microwave oven used in household and commercial kitchens is the main interference source in the 2.4 GHz unlicensed frequency band. The magnetron tubes used in the microwave ovens radiate a continuous-wave-like (CW-like) interference that sweeps over tens of megahertz (MHz) of the 2.4-2.483 GHz band during the positive half cycle of ac line voltage. The microwave oven‘s EIRP has a maximum ranging between 16 and 33 dBm. The power cycle frequency is 50 Hz 20 msec or 60 Hz 16 msec depending upon the geographical location. In North America, the ac line frequency is 60 HZ and the microwave oven‘s magnetron pulses on for 8msec and off for 8 msec. The maximum packet length defined in the IEEE 802.11 protocol was designed to operate between the 8 msec pulses of the microwave energy.

Other sources of interference include neighboring in-band radios that can be minimized by proper cell planning of the channel frequency and hopping patterns and careful layout of the APs. The second type of interference is from other systems such as neighboring DSSS and FHSS WLAN networks. Built into the standard are three mechanisms used to help minimize the amount of interference. The first is the clear channel assessment, where the MAC layer protocol provides a method of collision avoidance. The second is processing gain, which provides some protection from FHSS radios, whose spectrum appears as narrowband interferers. The third are the hop patterns; there is sufficient frequency spacing between pseudorandom hops to minimize the interference due to neighboring DSSS channels. To some degree, legacy 2.4 GHz IEEE 802.11-compliant FHSS and DSSS systems and IEEE 802.11b high-rate WLAN systems do coexist. However, careful cell planning will help minimize the amount of interference a system will experience especially at the outer fringe of the cell.

7.10 Antenna Diversity

Historically antenna diversity has been an effective low-cost alternative solution used to combat and mitigate the effects of multipath and delay spread in WLAN radio receivers. It is relatively easy to implement in the mobile stations and APs and does not require the signal processing hardware used in other diversity techniques. The object behind antenna diversity is to space the antennas apart from each other to minimize the effects of the uncorrelated multipath at the receiver. Spacing the antennas far apart allows the receiver to pick and demodulate the larger signal of the two signals. For 2.4 GHz IEEE 802.11 implementations, the bit length of the preamble sync fields was selected based on these criteria. The antennas are typically spaced anywhere from 0.25l to several lambdas (wavelengths) apart. The amount of separation depends upon the amount of delay-spread tolerance required for the system to operate in a given operating environment. Adding antenna diversity will improve the packet error rate (PER) performance of a wireless link by 2 or 1, as well as improve the availability of the link. There are a number of 2.4 GHz antennas on the market today with different

configurations. Patch antennas are commonly used at the mobile client PCMCIA implements, because of cost and size constraints. On the other hand, omni-directional antennas are used at the AP because they provide the optimal antenna coverage. Although antenna diversity is an option in the standard, as a minimum, antenna diversity should always be consider at the AP, as shown in Figure 7.1. This form of diversity will minimize the risk of packet loss due to multipath and interference, and ensure optimal throughput performance in a system.

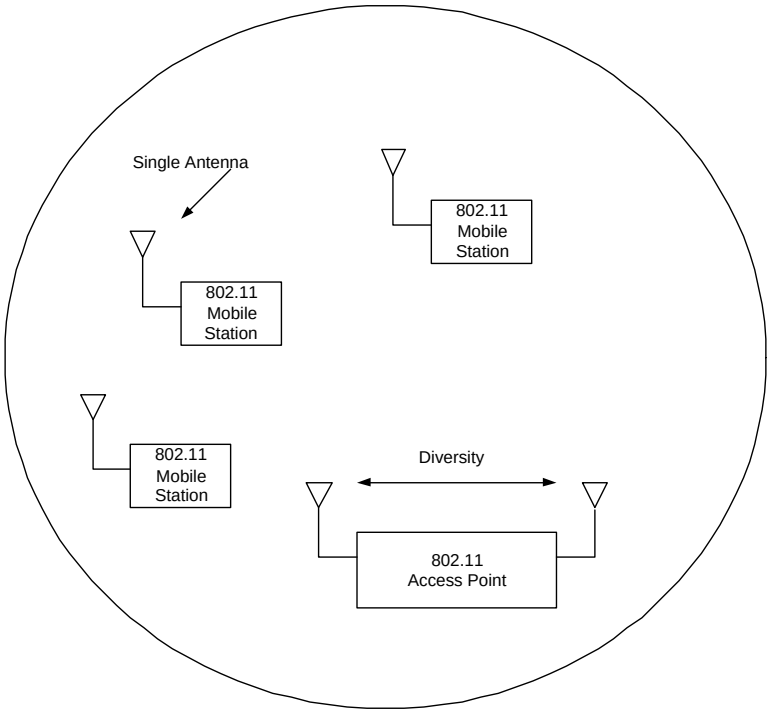


Figure 7.1: Antenna Diversity at the AP as a Minimum

Chapter 8

IEEE 802.11 PROTOCOLS

8.1 Overview of IEEE 802.11 Standards

In addition to the 802.11a and 802.11b , 802.11 standards are being developed that extend the physical layer options, **improve security**, **add quality of service (QoS)** features or provide better inter-operability. Vendors are likely to offer proprietary implementations of these features before the IEEE finalizes the standards.

IEEE 802.11a A physical layer standard for WLANs in the 5GHz radio band. It specifies eight available radio channels. Maximum link rate of 54-Mbps per channel. Comments: Higher data throughput and greater number of channels give better protection against possible interference from neighboring access points. When: Standard completed in 1999. Products are available now.

IEEE 802.11b A physical layer standard for WLANs in the 2.4 GHz radio band. It specifies three available radio channels. Maximum link rate of 11-Mbps per channel. Comments: Installations may suffer from speed restrictions in the future as the number of active users increase, and the limit of three radio channels may cause interference from neighboring access points. When: Standard completed in 1999. Products have been available since 2001.

IEEE 802.11d 802.11d is supplementary to the Media Access Control layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for user devices. The 802.11 standards cannot legally operate in some countries; the purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries. Comments: Equipment manufacturers do not want to produce a wide variety of country-specific products and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions. When: Work is ongoing, but see 802.11h for a timeline on 5 GHz WLANs in Europe.

IEEE 802.11e Supplementary to the MAC layer to provide QoS support for LAN applications. It will apply to 802.11 physical standards a,b and g. The purpose is to provide classes of service with managed levels

of QoS for data, voice and video applications. Comments: 11e should provide some useful features for differentiating data traffic streams. Many WLAN manufacturers have targeted QoS as a feature to differentiate their products, so there will be plenty of proprietary offerings before 11e is complete. *When:* The finalized standard is expected in the second half of 2002. Products will be available in the second half of 2003.

IEEE 802.11f This is a "recommended practice" document that aims to achieve radio access point interoperability within a multi-vendor WLAN network. The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another. *Comments:* 802.11f will reduce vendor lock-in and allow multi-vendor infrastructures. *When:* Completed standard expected in the second half of 2002. Products will be available in the first half of 2003.

IEEE 802.11g A physical layer standard for WLANs in the 2.4 GHz and 5 GHz radio band. It specifies three available radio channels. The maximum link rate is 54-Mbps per channel compared with 11 Mbps for 11b. The 802.11g standard uses OFDM modulation but, for backward compatibility with 11b, it also supports complementary code keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation. *Comments:* Speeds similar to 11a and backward compatibility may appear attractive but there are modulation issues: Conflicting interests between key vendors have divided support within IEEE task group for the OFDM and PBCC modulation schemes. The task group compromised by including both types of modulation in the draft standard. With the addition of support for 11b's CCK modulation, the end result is three modulation types. This is perhaps too little, too late and too complex compared with 11a. However, there are advantages for vendors looking to supply dual-mode 2.4 GHz and 5 GHz products, in that using OFDM for both modes will reduce silicon cost. *When:* Completed standard expected in the second half of 2002. Products will be available in the first half of 2003.

IEEE 802.11h This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar. *Comments:* Completion of 11h will provide better acceptability within Europe for IEEE compliant 5 GHz WLAN products. *When:* The standard is expected to be finalized by the second half of 2002. Products will be available in the first half of 2003.

IEEE 802.11i Supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a,b and g. It provides an alternative to WEP with new encryption methods and authentication procedures. IEEE 802.1x forms a key part of 802.11i. *Comments:* Security is a major weakness of WLANs. Weakness of WEP encryption is damaging the 802.11 standard perception in the market. Vendors have not improved matters by shipping products without setting default security features. In

addition, the WEP algorithm weakness have been exposed. The 11i specification is part of a set of security features that should address and overcome these issues by the end of 2002. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (an iterated block chipper) and TKIP backwards compatibility. *When:* Finalization of the TKIP protocol standard is expected in the first half of 2002. Firmware will be available in the second half of 2002. New silicon with an AES cipher is expected by the second half of 2003.

IEEE 802.11x A framework for regulating access control of client stations to a network via the use of extensible authentication methods. It forms a key part of the important 802.11i proposals for enhanced security. It applies to 802.11 physical standards a,b and g.

IEEE 802.1p A standard for traffic class and dynamic multicast filtering. It provides a method to differentiate traffic streams in priority classes in support of quality of service offering. It forms a key part of the 802.11e proposals for QoS at the MAC level. This applies to 802.11 physical standards a,b and g.

8.2 IEEE 802.11E MAC PROTOCOL

The IEEE 802.11e is an extension of the 802.11 Wireless Local Area Network (WLAN) standard for provisioning of Quality of Service (QoS). The new standard provides the means of prioritizing the radio channel access within an infrastructure *Basic Service Set (BBS)*of the IEEE 802.11 WLAN. A BSS that supports the new priority schemes of the 802.11e is referred to as QoS supporting BSS (QBSS).

There are enhancements to the 802.11 MAC currently under discussion, called the 802.11e, which introduce *Enhanced DCF (EDCF)* and *Hybrid Coordination Function (HCF)*. Stations, which operate under the 802.11e, are called QoS stations, and a QoS station, which works as the centralized controller for all other stations within the same QBSS, is called the *Hybrid Coordinator (HC)*. A QBSS is a BSS, which includes an 802.11e-compliant HC and QoS stations. The HC will typically reside within an 802.11e AP. In the following, we mean an 802.11e-compliant QoS station by a station. The EDCF is a contention-based channel access mechanism of HCF.

With 802.11e, there may still be the two phases of operation within the superframes, i.e., a CP (Contention Period and a CFP (Contention Free Period), which alternate over time continuously. The EDCF is used in the CP only, while the HCF is used in both phases, which makes this new coordination function hybrid.

8.2.1 Enhanced Distribution Coordination Function

The EDCF in 802.11e is the basic for the HCF. The QoS support is realized with the introduction of Traffic Categories (TCs). MSDUs are now delivered through multiple backoff instances within one station, each backoff instance parameterized with TC-specific parameters. In the CP, each TC within the stations contends for a TXOP and independently starts a backoff after detecting the channel being idle for an Arbitration Interframe space (AIFS), each backoff sets a counter to a random number drawn from the interval $[1, CW+1]$. The minimum size ($CWmin[TC]$) of the CW is another parameter dependent on the TC. Priority over legacy

stations is provided by setting $CWmin[TC] < 15$ (in case of 802.11a PHY) and $AIFS = DIFS$. See Figure 8.1 for illustration of the EDCF parameters.

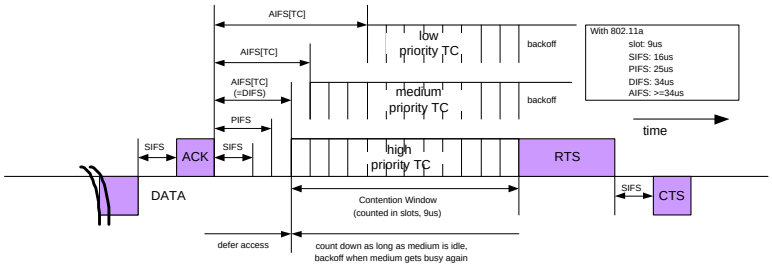


Figure 8.1: Multiple parallel backoffs of MSDUs with different priorities. Note that AIFS may be smaller than DIFS. In that case the CW starts at 1 rather than 0, which is the same as AIFS=DIFS.

As in the legacy DCF, when the medium is determined busy before the counter reaches zero, the backoff has to wait for the medium being idle for AIFS again, before continuing to count down the counter. A big difference from the legacy DCF is that when the medium is determined busy before the counter reaches zero, the backoff has to wait for the medium being idle for AIFS again, before continuing to count down the counter. A big difference from the legacy DCF is that when the medium is determined as being idle for the period of AIFS, the backoff counter is reduced by one beginning the last slot interval of the AIFS period. Note that with the legacy DCF, the backoff counter is reduced by one beginning the firs slot interval after the DIFS period. After any unsuccessful transmission attempt a new CW is calculated with the help of the persistence factor $PF[TC]$ and another uniformly distributed backoff counter out of this new, enlarged CW is drawn, to reduce the probability of a new collision. Whereas in legacy 802.11 CW is always doubled after any unsuccessful transmission (equivalent to PF=2), 802.11e uses the PF to increase the CW different for each TC:

$$newCW[TC] >= ((oldCW[TC] + 1) * PF) - 1$$

Thw CW never exceeds the parameter $CWmax[TC]$, which is the maximum possible value for CW.

A single station may implement up to eight transmission queues realized as virtual stations inside a station, with QoS parameters that determine their priorities. If the counters of two or more parallel TCs in a single station avoids the *virtual collision*. The scheduler grants the TXOP to the TC with highest priority, out of the TCs that virtually collided within the station, as illustrated in Figure 8.2. There is then still a possibility that the transmitted frame collides at the wireless medium with a frame transmitted by other stations.

Another important part of the 802.11e MAC is the *Transmission Opportunity (TXOP)*. A TXOP is an interval of time when a station has the right to initiate transmissions , defined by a starting time and a maximum duration. TXOPs are acquired via contention (EDCF-TXOP) or granted by the HC via polling (polled TXOP). The duration of an EDCF-TXOP is limited by a QBSS-wide *TXOP* limit distributed in beacon

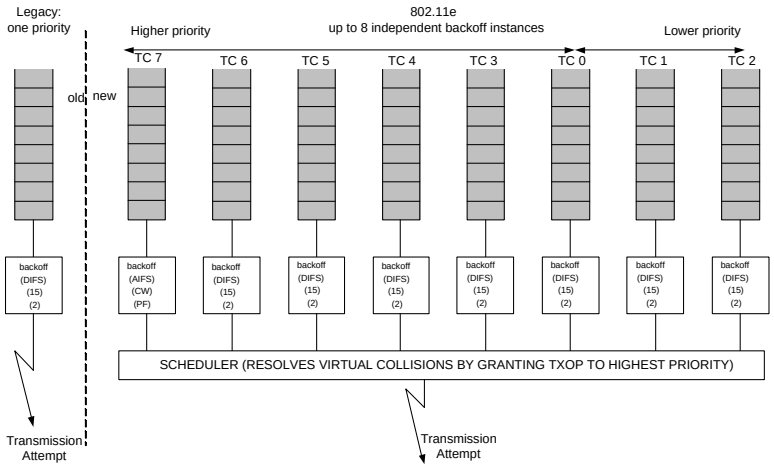


Figure 8.2: Virtual backoff of eight traffic categories: (1) left one: legacy DCF, close to EDCF with AIFS=34us, CWmin=15, PF=2; (2) right one: EDCF with AIFS[TC]=¿ 34us, CWmin[TC]=0-255,PF[TC]=1-16.

frames. While the duration of a polled TXOP is specified by the duration field inside the poll frame. However, although the poll frame is a new frame as part of the upcoming 802.11e, also the legacy stations set their NAVs upon receiving this frame. More details about polled TXOP follow in the next subsection. The prioritized channel access is realized with the QoS parameters per TC, which include AIFS[TC], CWmin[TC], and PF[TC]. CWmax[TC] is optional. There are discussions to introduce priority dependent EDCF-TXOP[TC]. The QoS parameters can be adapted over time by the HC, and will be announced periodically via the beacon frames. Protocol-related parameters are included in the beacon frame, which is transmitted at the beginning of each superframe.

8.2.2 Hybrid Coordination Function

The HCF extends the EDCF access rules. The HC may allocate TXOPs to itself to initiate MSDU Deliveries whenever it wants, however, only after detecting the channel as being idle for PIFS, which is shorter than DIFS. To give the HC priority over the EDCF, AIFS must be longer than PIFS and can therefore not have a value smaller than DIFS.

During CP, each TXOP begins either when the medium is determined to be available under the EDCF rules, i.e., after AIFS plus backoff time, or when the station receives a special poll frame, the QoS CF-Poll from the HC. The QoS CF-Poll from the HC can be sent after a PIFS idle period without any backoff. Therefore the HC can issue polled TXOPs in the CP using its prioritized medium access. During the CFP, the starting time and maximum duration of each TXOP is specified by the HC, again using the QoS CF-Poll frames. Stations will not attempt to get medium access on its own during the CFP, so only the HC can grant TXOPs by sending QoS CF-Poll frames. The CFP ends after the time announced in the beacon frame or by

a CF-End frame from the HC.

As part of 802.11e, an additional random access protocol that allows fast collision resolution is defined. The HC polls stations for MSDU Delivery. For this, the HC requires information that has to be updated by the polled stations form time to time. Controlled contention is a way for the HC to learn which station needs to be polled, at which times, and for which duration. The controlled contention mechanism allows stations to request the allocation of polled TXOPs by sending resource requests, without contending with other (E)DCF traffic. Each instance of controlled contention occurs during the controlled contention interval, which is started when the HC sends a specific control frame. This control frame forces legacy stations to set their NAV until the end of the controlled contention interval, thus they remain silent during the controlled contention interval. The control frame defines a number of controlled contention opportunities (i.e., short intervals seperated by SIFS) and a filtering mask containing the TCs in which resource requests may be placed. Each station with queued traffic for a TC matching the filtering mask chooses one opportunity interval and transmits a resource request frame containing the requested TC and TXOP duration, or the queue size of the requested TC. For fast collision resolution, the HC acknowledges the reception of request by generating a control frame with a feedback field so that the requesting stations can detect collisions during controlled contention.

The polled TXOPs are allocated with highest priority, without any CA, i.e. without any backoff before the poll. The polling scheme requires that there is one HC coordinating the channel, without any other HC in the range of this HC.

Bibliography

[1] B. O'Hara, A. Petrick, *"IEEE 802.11 Handbook- A Designer's Companion"*, IEEE Press.

[2] S. Mangold, L. Berlemann, G. Hiertz, *"QoS Support as Utility for Coexisting Wireless LANs"*, IPCN Paris,2002.

[3] IEEE 802.11 WG, *"Reference number ISO/IEC 8802-11:1999(E) IEEE Std 802.11, 1999 edition. International Standard [for] 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," 1999.*