CHAPTER

8

802.11 PHY Layers

CWAP Exam Objectives Covered:

- Explain PHY Layer terminology used in the 802.11 series of standards
- Describe the PLCP Layer (802.11a/b/g)
  - Purpose
  - Preambles and Headers
  - Payloads
- Describe the PMD Layer

In This Chapter

PHY Architecture

PHY Operations

DSSS PHY

ERP-OFDM PHY

DSSS-OFDM PHY

Transmit Procedure

Receive Procedure

Physical Layer Architecture

This section focuses on operation of items specified by the 802.11 series of standards for the physical layer. These items will include the PLCP and PMD sublayers, management layer entities, and generic management primitives. An in-depth understanding of how the physical layer operates and how it interfaces with the MAC layer is vitally important to the analyst's understanding of information gathered by a wireless protocol analyzer.

PLCP Sublayer

The MAC layer communicates with the Physical Layer Convergence Protocol (PLCP) sublayer via primitives (a set of "instructive commands" or "fundamental instructions") through a service access point (SAP). When the MAC layer instructs it to do so, the PLCP prepares MAC protocol data units (MPDUs) for transmission. The PLCP minimizes the dependence of the MAC layer on the PMD sublayer by mapping MPDUs into a frame format suitable for transmission by the PMD. The PLCP also delivers incoming frames from the wireless medium to the MAC layer. The PLCP sublayer is illustrated in Figure 8.1.

The PLCP appends a PHY-specific preamble and header fields to the MPDU that contain information needed by the Physical layer transmitters and receivers. The 802.11 standard refers to this composite frame (the MPDU with an additional PLCP preamble and header) as a PLCP protocol data unit (PPDU). The MPDU is also called the PLCP Service Data Unit (PSDU), and is typically referred to as such when referencing physical layer operations. The frame structure of a PPDU provides for asynchronous transfer of PSDUs between stations. As a result, the receiving station's Physical layer must synchronize its circuitry to each individual incoming frame.

PMD Sublayer

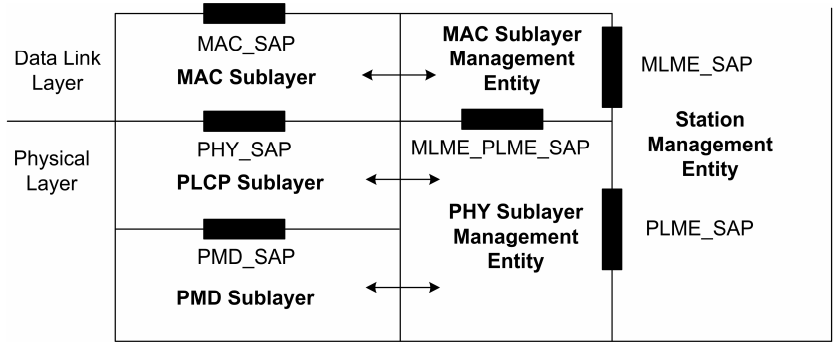
Under the direction of the PLCP, the Physical Medium Dependent (PMD) sublayer provides transmission and reception of Physical layer data units between two stations via the wireless medium. To provide this service,

the PMD interfaces directly with the wireless medium (that is, RF in the air) and provides modulation and demodulation of the frame transmissions. The PLCP and PMD sublayers communicate via primitives, through a SAP, to govern the transmission and reception functions. The PMD sublayer is illustrated in Figure 8.1.

Management Layer Entities

Both MAC and PHY layers conceptually include management entities, called the MAC sublayer management entity and the PHY sublayer management entity. These entities are referred to as the MAC Layer Management Entity (MLME), and the Physical Layer Management Entity (PLME). These entities provide the layer management service interfaces through which layer management functions may be invoked. In order to provide correct MAC operation, a station management entity (SME) shall be present within each station. The SME is a layer-independent entity that may be viewed as residing in a separate management plane or as residing "off to the side." The exact functions of the SME are not specified in the 802.11 standard, but in general this entity may be viewed as being responsible for such functions as the gathering of layer-dependent status from the various layer management entities, and similarly setting the value of layer-specific parameters. The SME would typically perform such functions on behalf of general system management entities and would implement standard management protocols. Figure 8.1 depicts the relationship among management entities.

FIGURE 8.1 802.11 Physical and MAC Layer Architecture



The various entities within this model interact in various ways. Particular interactions are defined explicitly within the 802.11 standard, via a service access point (SAP) across which defined primitives are exchanged. Other interactions are not defined explicitly within the 802.11 standard, such as the interfaces between MAC and MLME and between PLCP and PLME. The specific manner in which these MAC and PHY management entities are integrated into the overall MAC and PHY layers is not specified within the 802.11 standard.

Generic Management Primitives

The management information specific to each layer is represented as a management information base (MIB) for that layer. The MAC and PHY layer management entities are viewed as "containing" the MIB for that layer. The generic model of MIB-related management primitives exchanged across the management SAPs is to allow the SAP user-entity to either GET the value of a MIB attribute, or to SET the value of a MIB attribute.

The practical usage example of management primitives is when the user configures an access point or a mobile station's wireless utilities. This is done through a configuration interface such as CLI, GUI, SNMP, or custom software. Configuration of the access point's features through its web interface, for example, will SET a MIB attribute value to perhaps true/false or to some logical value.

Physical Layer Service Primitives

Due to lack of direct relevance of PHY service primitives to protocol analysis, they will not be explained in detail in this text. For more information on PHY primitives, refer to 802.11-1999 (R2003), Clause 12. There will be occasional references to these primitives within this text, but learning about primitives themselves is not relevant for the CWAP exam.

Physical Layer Operations

The general operation of the various Physical layers is very similar. To perform PLCP functions, the 802.11 standard specifies the use of state machines. Each state machine performs one of the following functions:

- Carrier Sense/Clear Channel Assessment (CS/CCA)
- Transmit (Tx)
- Receive (Rx)

Carrier Sense/Clear Channel Assessment (CS/CCA)

Carrier Sense/Clear Channel Assessment is used to determine the state of the medium. The CS/CCA procedure is executed while the receiver is turned on and the station is not currently receiving or transmitting a packet. The CS/CCA procedure is used for two specific purposes: to detect the start of a network signal that can be received (CS) and to determine whether the channel is clear prior to transmitting a packet (CCA).

Transmit (Tx)

Transmit (Tx) is used to send individual octets of the data frame. The transmit procedure is invoked by the CS/CCA procedure immediately upon receiving a PHY-TXSTART.request (TXVECTOR) from the MAC sublayer. The CSMA/CA protocol is performed by the MAC with the PHY PLCP in the CS/CCA procedure prior to executing the transmit procedure.

Receive (Rx)

Receive (Rx) is used to receive individual octets of the data frame. The receive procedure is invoked by the PLCP CS/CCA procedure upon detecting a portion of the preamble sync pattern followed by a valid SFD and PLCP Header. Although counter-intuitive, the preamble and PLCP header are not “received”. Only the MAC frame is “received”.

The following sections describe how each of the PLCP functions is used for transferring data between the MAC and Physical layers.

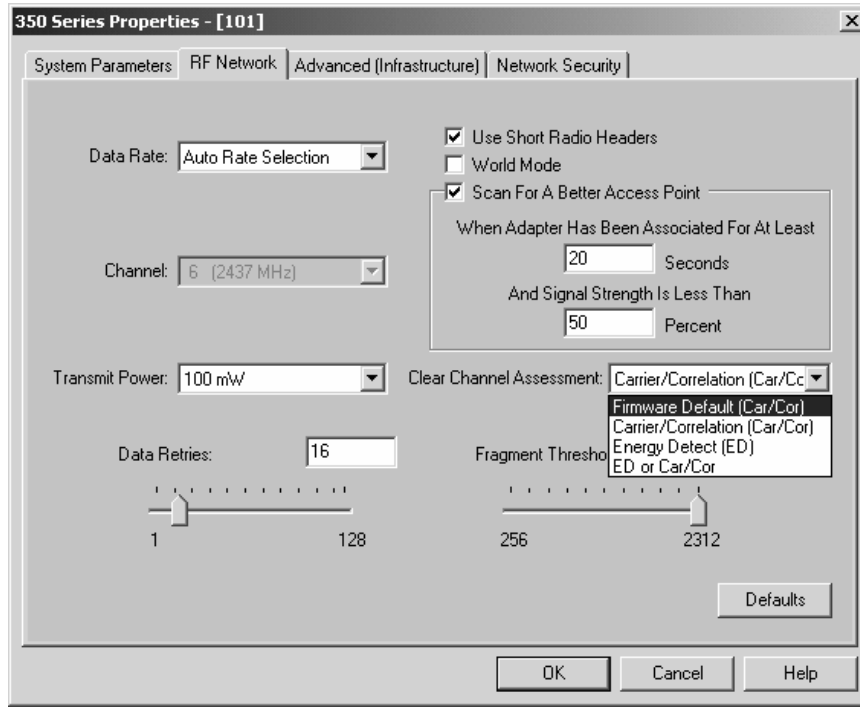
Carrier Sense Function

The Physical layer implements the carrier sense operation by directing the PMD to check to see whether the medium is busy or idle. The PLCP performs the following sensing operations if the station is not transmitting or receiving a frame:

- *Detection of incoming signals* - The PLCP within the station will sense the medium continually. When the medium becomes busy, the PLCP will read in the PLCP preamble and header of the frame to attempt synchronization of the receiver to the data rate of the signal.
- *Clear channel assessment* - The clear channel assessment operation determines whether the wireless medium is busy or idle. If the medium is idle, the PLCP will send a *PHY-CCA.indicate* primitive (with its status field indicating idle) to the MAC layer. If the medium is busy, the PLCP will send a *PHY-CCA.indicate* primitive (with its status field indicating busy) to the MAC layer. The MAC layer can then make a decision on whether to send a frame.

Stations and access points that are 802.11-compliant store the clear channel assessment operating mode in the Physical layer MIB attribute *aCCAModeSuprt*. A developer can set this mode through station initialization procedures. Figure 8.2 shows an example of configuring the different CCA operating modes.

FIGURE 8.2 Configuring CCA Operating Modes on a Mobile Station



Transmit Function

The PLCP will switch the PMD to transmit mode after receiving the *PHY-TXSTART.request* primitive from the MAC layer. The MAC layer sends the number of octets (0-4095) and the data rate instruction along with this request. The PMD responds by sending the preamble of the frame at the antenna within 20 microseconds.

Multicast and broadcast frames are generally sent at the lowest basic data rate.

The transmitter sends the preamble at 1 Mbps (802.11 or 802.11b DSSS) or 6 Mbps (802.11a or 802.11g ERP-OFDM). The PHY header is then sent at 1 Mbps (802.11 or 802.11b DSSS) when long preambles are in

use, 2 Mbps (802.11b DSSS) when short preambles are in use, or 6 Mbps (802.11a or 802.11g OFDM) when fixed 12-symbol OFDM preambles are in use. These are the lowest supported rates for each PHY and provide a specific common data rate at which receivers listen. After sending the header, the transmitter changes the data rate of the transmission to what the header specifies for transmitting the PSDU. After the PSDU transmission takes place, the PLCP sends a *PHY-TXSTEND.confirm* primitive to the MAC layer, shuts off the transmitter, and switches the PMD circuitry to receive mode.

Receive Function

If the clear channel assessment discovers a busy medium and valid preamble (Sync & SFD) of an incoming frame, the PLCP will monitor the header of frame. The PMD will indicate a busy medium when it senses a signal having a power level of at least -85 dBm. If the PLCP determines the header is error free, the PLCP will send a *PHY-RXSTART.indicate* primitive to the MAC layer to provide notification of an incoming frame. The PLCP sends the information it finds in the frame header (such as the number of octets and data rate) along with this primitive.

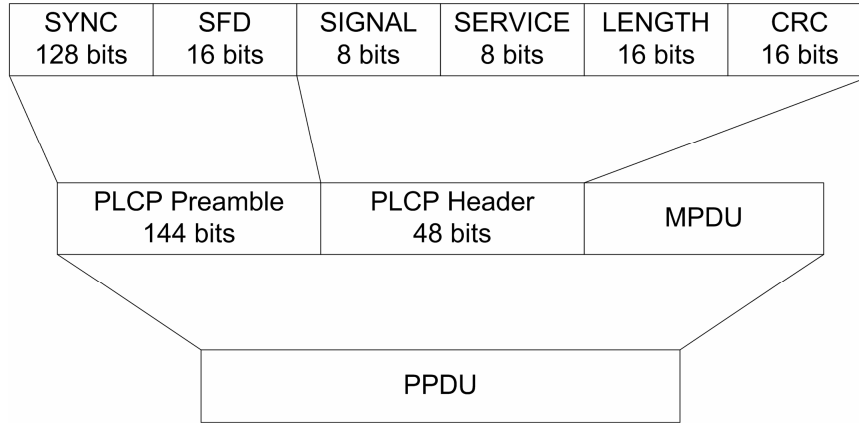
The PLCP sets an octet counter based on the value in the PPDU header's Length field (discussed later in this section). This counter will keep track of the number of PSDU octets received, enabling the PLCP to know when the end of the frame occurs. As the PLCP receives data, it sends octets of the PSDU to the MAC layer via *PHY-DATA.indicate* messages. After receiving the final octet, the PLCP sends a *PHY-RXEND.indicate* primitive to the MAC layer to indicate the final octet of the frame.

The receive function will operate with single or multiple antenna diversities. You can select the level of diversity (that is, the number of antennas) via access point and radio card parameters. The strength of the transmitted signal decreases as it propagates to the destination. Many factors, such as the distance, heat, rain, fog, and obstacles may cause this signal degradation. Multipath propagation can also lessen the signal strength at the receiver. Diversity is a method of improving reception by receiving the signal on multiple antennas and processing the superior signal.

DSSS PHY

The IEEE 802.11b Direct Sequence Spread Spectrum (DSSS) Physical layer delivers frames at 1, 2, 5.5, and 11 Mbps rates in the 2.4 GHz ISM band. The original 802.11 Clause 15 DSSS standard specified only 1 and 2 Mbps data rates using only long preambles. The only coding/modulation used in 802.11 Clause 15 is Barker code with DBPSK (1 Mbps) and DQPSK (2 Mbps). Figure 8.3 illustrates the construction of the DSSS PLCP Protocol Data Unit (PPDU), which includes a long preamble, the header, and the MPDU (PSDU) as specified in the 802.11 standard. The preamble and the header are both transmitted at 1 Mbps when using the long preamble format. The MPDU is transmitted at the data rate specified by the transmitting station (or access point). The preamble enables the receiver to synchronize to the incoming signal properly before the actual content of the frame arrives. The header provides information about the frame, and the PSDU is the MPDU the transmitting station is sending.

FIGURE 8.3 DSSS PPDU, 802.11-1999 (R2003)



The 802.11b standard further specifies rates of 5.5 and 11 Mbps, each using CCK modulation. The option of a short preamble was introduced in the 802.11b standard, giving the administrator two configuration options.

Figure 8.4 illustrates the same DSSS PPDU specified in the 802.11 standard, but with the newly supported MPDU data rates.[1]

FIGURE 8.4 802.11b, DSSS PPDU, Long Preamble

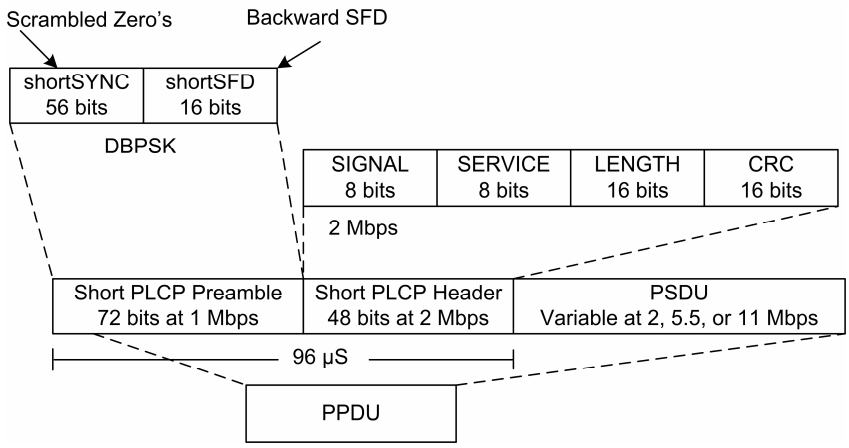
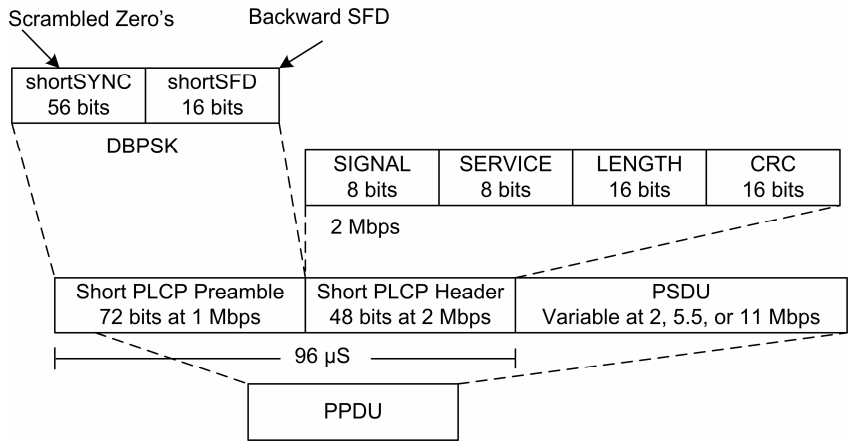


Figure 8.5 illustrates the optional 802.11b DSSS PPDU with the short preamble.[2] Instead of scrambled 1s found in the long preamble Sync field, scrambled 0s are used. The Sync field is only 56 bits instead of the 128 in the original PPDU. The SFD field is presented in reverse bit order. The preamble is transmitted at 1 Mbps, the header at 2 Mbps, and the PSDU (MPDU) at the data rate specified by the transmitting station (or access point). DSSS PPDUs transmitted using short preambles only support PSDU data rates of 2, 5.5, and 11 Mbps.

[1] 802.11b – 1999 (Cor 2001), Section 18.2.2.1
[2] 802.11b – 1999 (Cor 2001), Section 18.2.2.2

FIGURE 8.5 802.11b, DSSS PPDU, Short Preamble



DSSS Preamble

The preamble is the first of three parts of a PPDU. The preamble consists of two parts: The Synchronization (Sync) field and Start Frame Delimiter (SFD) field.

The Sync field consists of a string of 0s or 1s, alerting the receiver that a potentially receivable signal is present. A receiver will begin to synchronize with the incoming signal after detecting the Sync. Consider that receivers may not receive the entire Sync field, but rather only catch part of it. Since the Sync field is a continuous stream of 0s or 1s, it really does not matter where in the stream the receiver realizes that there is a Sync signal being transmitted so long as it synchronizes before the SFD arrives.

The Start Frame Delimiter field defines the beginning of a frame. The bit pattern for this field is always 1111001110100000 when using long preambles and reversed when using short preambles. These patterns are unique to the DSSS PLCP.

Starting with 802.11b, short preambles were optional, and there were various implementations of short preambles in the market. For example,

some access points implemented short preambles as, “short preambles only.” Other access points implemented short preambles as “short or long preambles are ok.” In a, “short preambles only” implementation where the access point is configured for short preambles, a station using long preambles will not be able to associate. In a, “short or long preambles are ok” implementation where the access point is configured for short preambles, stations using either long or short preambles may associate, but the lowest common denominator (long preambles) is always used in the BSS. This is to say that if a long preamble station enters the BSS, the access point will declare that all stations must now use long preambles.

The 802.11g standard made support of both long and short preambles mandatory, such that all implementations where the access point has short preambles enabled mean, “short or long preambles are ok.” To see whether the access point has enabled short preamble support, see the *Short Preamble* bit of the Capability Information fixed field.

Beacons & Probe Responses

When only ERP stations are present in the BSS, the access point uses an OFDM PHY (and thus OFDM preambles) for the beacon frames. When a NonERP station associates to the BSS, the access point uses the DSSS PHY (and thus DSSS preambles) for the beacon frames. When the NonERP stations are all short-preamble capable, the access point sends the beacon with a short preamble. When any of the NonERP stations are long-preamble-only capable, the access point sends the beacon using a long preamble. When a NonERP station sends a probe request frame to the access point using a long preamble, the access point must reply with a probe response frame using a long preamble. When a NonERP station sends a probe request frame to the access point using a short preamble, the access point must reply with a probe response frame using a short preamble. This is sometimes considered the “preamble echo” rule, though it is not called by this name in the 802.11 series of standards.

DSSS Header

Signal Field

The Signal field identifies the type of modulation that the receiver must use to demodulate the signal. The value of this field is equal to the data rate divided by 100 Kbps. The only two possible values allowed in the original 802.11 standard were:

Data Rate	Signal Field Value
1Mbps	00001010
2Mbps	00010100

For 802.11 b, the four possible values were:

Data Rate	Signal Field Value
1Mbps	00001010
2Mbps	00010100
5.5Mbps	00110111
11Mbps	01101110

Regardless of the rate or preamble used with DSSS-OFDM the Signal field is set to a 3 Mbps value. That is, the eight-bit value is set to 00011110. With DSSS-OFDM, an optional 802.11g PHY, this value is simply a default setting used for BSS compatibility and to ensure that NonERP stations read the length field and defer the medium for that amount of time even though they cannot demodulate the MPDU due to unsupported rates.

Service Field (802.11 & 802.11b)

The 802.11 standard reserves the Service field for future use; however, a value of 00000000 means 802.11 compliance.[1] The 802.11b standard made use of the Service field as shown in Figure 8.6.[2]

[1] 802.11–1999 (R2003), Section 15.2.3.4
[2] 802.11b – 1999 (Cor 2001), Section 18.2.3.4

FIGURE 8.6 802.11b Service Field

b0	b1	b2	b3	b4	b5	b6	b7
Reserved	Reserved	Locked clocks bit 0 = not locked 1 = locked	Modulation Selection bit 0 = CCK 1 = PBCC	Reserved	Reserved	Reserved	Length extension bit

Bit 7 (is used to extend the Length header field). Since both PBCC, an optional modulation type specified in 802.11b and 802.11g, and CCK modulations are supported in 802.11b, bit 3 is used to indicate whether PBCC or CCK is in use. Bit 2 is used to indicate that the transmit frequency and symbol clocks are derived from the same oscillator. This *Locked Clock* bit is set by the PHY layer based on its implementation configuration.

Service Field (802.11g)

Three bits of the Service field have been defined to support the optional modes of the 802.11g standard.[1] Figure 8.7 illustrates the bits within the Service field. Bits b0, b1, and b4 are reserved and are set to 0. Bit b2 is used to indicate that the transmit frequency and symbol clocks are derived from the same oscillator, the same as with 802.11b. For all ERP systems, the Locked Clock Bit is set to 1. Bit b3 is used to indicate if the data is modulated using the optional ERP-PBCC modulation. Bit b3 is defined in section 18.2.3.4 of the 802.11b standard with the caveat that the ERP-PBCC mode now has the additional optional rates of 22 and 33 Mbps in the 802.11g standard.[2] Bits b5, b6, and b7 are used to resolve data field length ambiguities for the optional ERP-PBCC-11, ERP-PBCC-22, and ERP-PBCC-33 modes. These bits are fully defined in 802.11g, Section 19.6. Bit b7, the Length Extension Bit, is also used to resolve data field length ambiguities for the CCK 11 Mbps per 802.11b, Section 18.2.3.5. Bits b3, b5, and b6 are set to 0 for CCK.

[1] 802.11g – 2003, Section 19.3.2.1
[2] 802.11g – 2003, Section 19.3.3.2

FIGURE 8.7 802.11g DSSS-OFDM Service Field

b0	b1	b2	b3	b4	b5	b6	b7
Reserved	Reserved	Locked clocks bit 0 = not locked 1 = locked	Modulation Selection bit 0 = Not ERP-PBCC 1 = PBCC	Reserved	Length extension bit (ERP-PBCC)	Length extension bit (ERP-PBCC)	Length extension bit

Length Field

OFDM PHYs treat the Length field as number of octets to transfer between MAC and PLCP as stated above. The DSSS and DSSS-OFDM PHYs are different and treat the Length field as number of microseconds required to transmit the PSDU. The DSSS and DSSS-OFDM PHYs calculate the Length field based on the number of octets presented by the MAC to the PLCP. Note that the length extension bits in the Signal field are not needed or used for DSSS-OFDM. Radio receivers spend most of their time doing carrier sense and clear channel assessment (CS/CCA). If the DSSS PHY header is successfully decoded, the receiver knows how long to spend receiving the rest of this frame. If the signal drops or is otherwise corrupted during that time, CS/CCA alone might conclude that the channel has returned to idle when in fact another station in a better position to receive is still successfully receiving. This means that the DSSS PHY header's Length field is effectively telling the MAC layer how long to consider the medium busy.

The DSSS PHY header's Length field will never show up on a protocol analyzer. It is unrelated to the duration field and NAV timers at the MAC layer.

In packetized RF data transmissions systems, transmitted messages are susceptible to various types of bit errors due to noise, interference, data collisions, and multipath in a given RF channel. The main purpose of error detection algorithms is to enable an RF receiver of a transmitted message to determine if the message is corrupted. There are various types of error detection algorithms to choose from. The most common method for detecting bit errors in messages is through the use of CRCs (Cyclic Redundancy Codes). CRCs are very useful in detecting single bit errors, multiple bit errors, and burst errors in packetized messages. In theory

CRCs could be thought of as simply taking a binary message and dividing it by a fixed binary number, with the remainder being the checksum, or more commonly the CRC. The CCITT CRC-16 is a standardized algorithm with origins to the CCITT standards body. The Signal, Service, and Length fields are all protected with a CCITT CRC-16 frame check sequence (FCS). The CRC operation is done at the transmitting station before scrambling. The Physical layer does not determine whether errors are present within the PSDU. CRC-16 detects all single and double-bit errors and ensures detection of 99.998% of all possible errors. Most experts feel CRC-16 is sufficient for data transmission blocks of 4 kilobytes or less.

DSSS PMD Sublayer

The DSSS PMD performs the actual transmission and reception of PPDUs under the direction of the PLCP. To provide this service, the PMD interfaces directly with the wireless medium (that is, RF in the air) and provides DSSS modulation and demodulation of the frame transmissions.

With direct sequence, the PLCP and PMD communicate via primitives, enabling the DSSS PLCP to direct the PMD when to transmit data, change channels, receive data from the PMD, and so on. The operation of the DSSS PMD translates the binary representation of the PPDUs into a radio signal suitable for transmission. The DSSS Physical layer performs this process by multiplying a radio frequency carrier by a pseudo-noise (PN) digital signal. The resulting signal appears as noise if plotted in the frequency domain. The wider bandwidth of the direct sequence signal enables the signal power to drop below the noise threshold without loss of information.

ERP-OFDM PHY

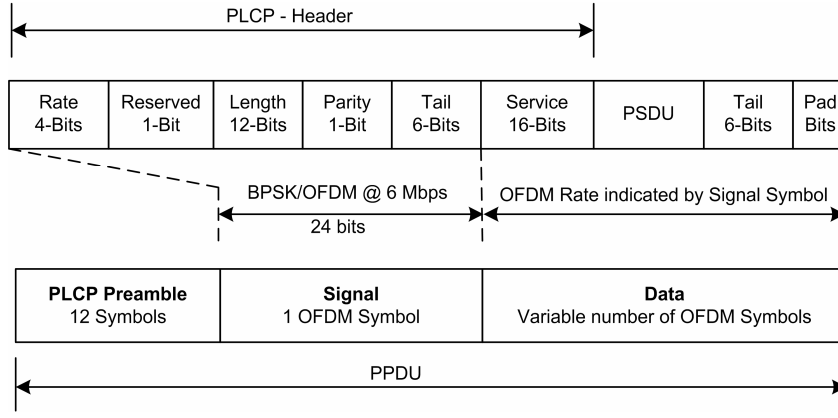
The two IEEE 802.11 Orthogonal Frequency Division Multiplexing (OFDM) Physical layers each deliver up to 54 Mbps data rates in the 2.4 GHz (802.11g) and 5GHz (802.11a) bands respectively. This section describes the architecture and operation of 802.11 OFDM.

The benefits of OFDM are high spectral efficiency, resiliency to RF interference, and lower multipath distortion. The orthogonal nature of OFDM allows subchannels to overlap, having a positive effect on spectral efficiency. The subcarriers transporting information are just far enough apart to avoid interfering with each other, theoretically.

ERP-OFDM PPDU

Figure 8.8 illustrates the format of an ERP-OFDM PPDU, used both in 802.11a[1] and 802.11g[2]. This is the only PLCP that 802.11a specifies, but one of several specified in the 802.11g standard. ERP-OFDM is, by far, the most often implemented PPDU in the 802.11g standard, and supports data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. The ERP-OFDM PPDU has three parts: Preamble, Header, and Data Field.

FIGURE 8.8 ERP-OFDM PPDU (802.11a/g)



ERP-OFDM PPDU Preamble

The ERP-OFDM PPDU Preamble (Sync) enables the receiver to acquire an incoming OFDM signal (signal detect) and synchronize its demodulator. The preamble consists of 12 training symbols[3], ten of which are short and are used for establishing AGC (automatic gain

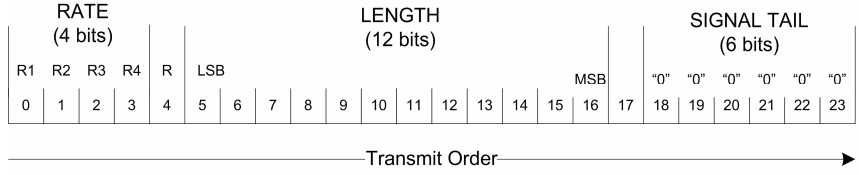
[1] 802.11a – 1999, Section 17.3.2
[2] 802.11g – 2003, Section 19.3.2.3
[3] 802.11a – 1999, Section 17.3.3

control), diversity selection, and the coarse frequency offset estimate of the carrier signal. The receiver uses the two long training symbols for channel and fine frequency offset estimation. With the ERP-OFDM preamble, it takes up to 16 microseconds to train the receiver after first detecting a signal on the RF medium.

ERP-OFDM PPDU Header

The ERP-OFDM Header consists of 4 rate bits, 1 reserved bit, 12 Length bits, 1 Parity bit, 6 Tail bits, and 16 Service bits. The Signal field is one symbol (24 bits) long, is not scrambled, and has the same contents as the entire PPDU header minus the Service subfield (16 bits). The Signal field is always transmitted at 6 Mbps using BPSK modulation. This section outlines the significance of each subfield within the Signal field and PPDU Header.

FIGURE 8.9 ERP-OFDM PPDU Header



The Rate subfield consists of 4 bits as outlined in Figure 8.10, and indicates the modulation and coding rate of the rest of the PPDU, starting immediately after the Signal field.

FIGURE 8.10 ERP-OFDM PPDU Rate Subfield

Bits 1-4	Data Rate	Modulation
1101	6 Mbps	BPSK
1111	9 Mbps	BPSK
0101	12 Mbps	QPSK
0111	18 Mbps	QPSK
1001	24 Mbps	16QAM
1011	36 Mbps	16QAM
0001	48 Mbps	64QAM
0011	54 Mbps	64QAM

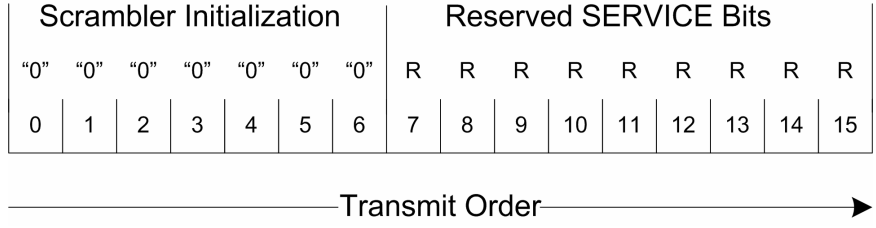
Some 802.11a chipset manufacturers are using proprietary techniques to combine OFDM channels for applications requiring data rates that exceed 54 Mbps.

The Reserved subfield (1 bit) is set to 0 since it is currently unused. The Length subfield (12 bits) indicates the number of octets in the PSDU that the MAC is currently requesting the PHY to transmit. The Parity subfield is a one bit positive (even) parity bit, based on the first 17 bits (0-16) of the frame (Rate, Reserved, and Length subfields). The Signal Tail subfield is 6 bits, each of which is always set to 0.

ERP-OFDM PPDU Data Field

The Data field consists of the Service subfield, PSDU, Tail subfield, and Pad Bits subfield. The Service subfield consists of 16 bits, with the first 7 bits as zeros to synchronize the descrambler in the receiver. The remaining 9 bits are reserved for future use and set to all 0s. As part of the Data field[1], the Service subfield is transmitted at the rate specified in the Signal field's Rate subfield.

FIGURE 8.11 ERP-OFDM PPDU Service Field



The PSDU is the data unit being sent down from the MAC layer for transmission on the wireless medium. The PSDU is transmitted at the data rate specified in the Signal field's Rate subfield and has a maximum length of 4095 octets[2].

The PPDU Tail subfield is 6 bits of 0, which are required to return the convolutional encoder to the "zero state." This procedure improves the

[1] 802.11a – 1999, Section 17.3.5
[2] 802.11a – 1999, Section 17.5.2, Table 93

error probability of the convolutional decoder, which relies on future bits when decoding and which may be not be available past the end of the message. The Tail field is produced by replacing six scrambled "zero" bits following the message end with six non-scrambled "zero" bits.

The Pad Bits subfield contains at least six bits, but it is actually the number of bits that make the Data field a multiple of the number of coded bits in an OFDM symbol (48, 96, 192, or 288).

A data scrambler using a 127-bit sequence generator scrambles all bits in the data field to randomize the bit patterns in order to avoid long streams of ones and zeros. Long streams of ones or zeros may create a DC bias voltage in the receiver circuitry, which may result in receiver errors. The data scrambler "balances" the number of ones and zeros being transmitted between stations.

ERP-OFDM PMD Sublayer

The ERP-OFDM PMD performs the actual transmission and reception of PPDUs under the direction of the PLCP. To provide this service, the PMD interfaces directly with the wireless medium and provides OFDM modulation and demodulation of the frame transmissions.

With ERP-OFDM, the PLCP and PMD communicate via primitives, enabling the DSSS PLCP to direct the PMD when to transmit data, change channels, receive data from the PMD, and so on. The operation of the ERP-OFDM PMD translates the binary representation of the PPDUs into a radio signal suitable for transmission. The ERP-OFDM Physical layer performs this process by dividing a high-speed serial information signal into multiple lower-speed sub-signals that the system transmits simultaneously at different frequencies in parallel.

DSSS-OFDM PHY

The 802.11g standard extended use of the DSSS PHY by specifying an optional PPDU type consisting of the same DSSS preamble and header, but accepting an ERP-OFDM PPDU as its PSDU. The IEEE calls this new PPDU type DSSS-OFDM. Both long and short preambles are supported with DSSS-OFDM, and no protection mechanisms are required

by DSSS-OFDM stations when operating with DSSS stations present in the BSA. Figures 8.12 and 8.13 illustrate the construction of both long and short preamble format DSSS-OFDM PPDUs. The preamble and header transmission rates apply to DSSS-OFDM as with DSSS.

FIGURE 8.12 802.11g, DSSS-OFDM PPDU, Long Preamble

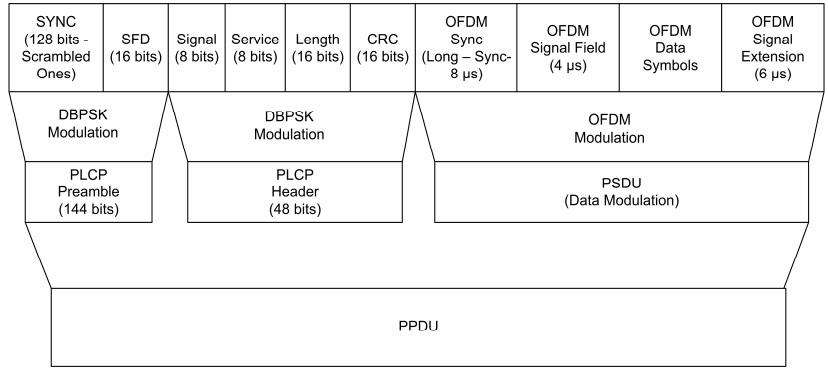
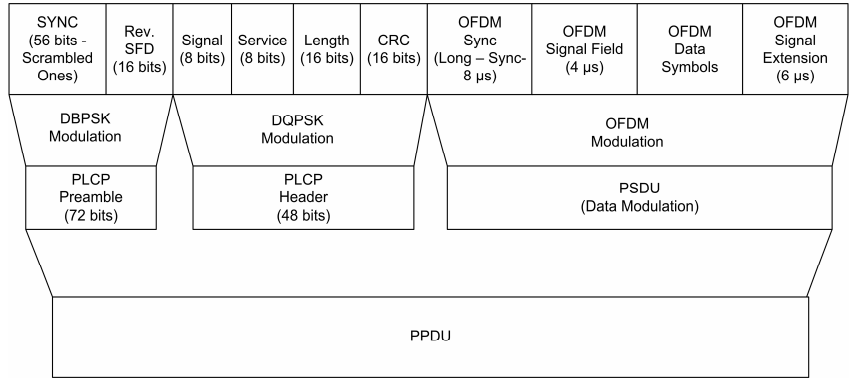
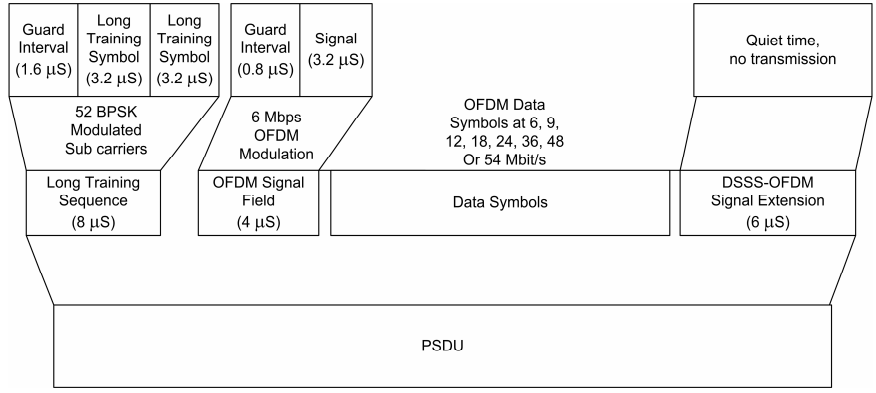


FIGURE 8.13 802.11g, DSSS-OFDM PPDU, Short Preamble



This section illustrates the format of the PSDU portion of the DSSS-OFDM PPDU. Figure 8.14 shows an expanded view of the DSSS-OFDM PSDU.

FIGURE 8.14 DSSS-OFDM PSDU Format



The PSDU is composed of four major sections. The first is the long sync training sequence that is used for acquisition of receiver parameters by the OFDM demodulator. The long sync training sequence for DSSS-OFDM is identical to the long training symbols of the 802.11a and 802.11g ERP-OFDM preamble. The second section is the OFDM Signal field that provides the demodulator information on the OFDM data rate and length of the OFDM data section. The Signal field for DSSS-OFDM is identical to the Signal field found in an 802.11a or 802.11g ERP-OFDM header. After the Signal field is the Data section of the PSDU. This section is modulated in the same way as any 802.11a or 802.11g ERP-OFDM PSDU. After the Data section, the PSDU for DSSS-OFDM appends a signal extension section to provide additional processing time for the OFDM demodulator. The DSSS-OFDM Signal Extension is a period of no transmission of 6 µs length. It is inserted to allow more time to finish the convolutional decoding of the OFDM segment waveform and still meet the 10 µs SIFS requirement of the ERP.

Transmit Procedure (802.11g)

The transmit procedure depends on the data rate and modulation format requested. For data rates of 1, 2, 5.5, 11, 22, and 33 Mbps, the PLCP transmit procedure is the same as for 802.11b. For the ERP-OFDM mandatory rates of 6, 12, and 24 and the optional rates of 9, 18, 36, 48, and 54 Mbps the PLCP transmit procedure is the same as for 802.11a. The transmit procedures for the optional DSSS-OFDM mode using the

long or short PLCP preamble and header are the same as those described in 802.11b for the preamble and header and 802.11a for the PSDU.

Receive Procedure (802.11g)

An ERP receiver should be capable of receiving 1, 2, 5.5, and 11 Mbps PLCPs using either the long or short preamble formats described in 802.11b, and should be capable of receiving 6, 12, and 24 Mbps using the modulation and preamble described in 802.11a. The PHY may also implement the ERP-PBCC modulation at rates of 5.5, 11, 22, and 33 Mbps; the ERP-OFDM modulations at rates of 9, 18, 36, 48, and 54 Mbps; and/or the DSSS-OFDM modulation rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. A receiver should be capable of detecting the preamble type (ERP-OFDM, Short Preamble, or Long Preamble) and the modulation type. Upon the receipt of a PPDU, the receiver should first distinguish between the ERP-OFDM preamble and the single carrier modulations (long or short preamble). In the case where the preamble is an ERP-OFDM preamble, the PLCP receive procedure should follow that of the 802.11a standard. Otherwise, the receiver should then distinguish between the long preamble and short preamble as specified in the 802.11b standard. The receiver should then demodulate the Service field to determine the modulation type. For short preamble and long preamble using DSSS, CCK, or PBCC modulations, the receiver should then follow the receive procedure described in 802.11b.

A receiver that supports DSSS-OFDM is capable of receiving all rates specified by 802.11 DSSS (1 & 2 Mbps) and all mandatory rates in 802.11a (6, 12, & 24 Mbps) and 802.11b (1, 2, 5.5, & 11 Mbps). If the Signal field indicates 3 Mbps, the receiver should attempt to receive a DSSS-OFDM frame. The remaining receive procedures for a DSSS-OFDM-capable receiver are the same as those described in 802.11b, and they do not change apart from the ability to receive DSSS-OFDM in the PSDU.

Summary

The 802.11 series of physical layer specifications includes a variety of options that govern the transmission and reception of frames. There are several 802.11 series PHYs, such as FHSS, DSSS, HR-DSSS, ERP-OFDM, DSSS-OFDM, and ERP-PBCC. Each PHY layer has a particular PLCP, which defines framing, and PMD that defines signal modulation. Understanding the differences and interactions between each PHY will allow the analyst to better design, baseline, and troubleshoot WLANs of various types, even in mixed environments.

Key Terms

Before taking the exam, you should be familiar with the following terms:

Direct Sequence Spread Spectrum (DSSS)

DSSS-OFDM

ERP-OFDM

Frequency Shift Keying (FSK)

long preamble

Orthogonal Frequency Division Multiplexing (OFDM)

PLCP Header

Physical Layer Convergence Procedure (PLCP)

Physical Layer Service Primitives

Physical Medium Dependent (PMD)

Quadrature Amplitude Modulation (QAM)

service primitives

short preamble

Review Questions

1. The MAC sublayer and the PLCP sublayer coordinate transmission of frames to and from the wireless medium using what?

2. An ERP-OFDM PPDU is comprised of what three parts?

3. In the DSSS PLCP header, what purpose does the length field serve?

4. When a short-preamble-capable NonERP station associates with an 802.11g access point while all other stations are ERP-OFDM capable, what PHY does the access point use for transmitting beacons?

5. The scrambler and descrambler serve what purpose in wireless LAN transmitters and receivers?

6. An ERP-OFDM Preamble uses how many symbols for training the receiver?

7. When transmitting a DSSS PSDU across the wireless medium using short preambles, what is the lowest supported data rate for the PSDU?

8. A DSSS PLCP header is protected from in-transit bit-flipping attacks by which field?

9. DSSS-OFDM supports what two preamble lengths?

10. An ERP-OFDM header is transmitted at what data rate?