CHAPTER 11

WIRELESS LAN TECHNOLOGY

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- Explain the roles of the layers in the IEEE 802.11 architecture.
- Describe the services provided by IEEE 802.11.
- Explain the use of backoff, interframe spacing, point coordination, and distributed coordination for MAC layer operation of IEEE 802.11.
- Describe the main methods used to improve throughput in IEEE 802.11n, 802.11ac, and 802.11ad.
- Explain the IEEE 802.11i WLAN security procedures.

Wireless LANs (WLANs) play an important role in the local area network market. Increasingly, organizations are finding that wireless LANs are an indispensable adjunct to traditional wired LANs, to satisfy requirements for mobility, relocation, ad hoc networking, and coverage of locations difficult to wire. In addition, a plethora of wireless devices use WLANs as a replacement for cellular coverage when in range (usually indoors) or as their main source of wireless connectivity.

This chapter provides a survey of wireless LANs. We begin with an overview that looks at the motivations for using wireless LANs and summarizes the various approaches in current use.

11.1 OVERVIEW AND MOTIVATION

As the name suggests, a wireless LAN is one that makes use of a wireless transmission medium for a local area network. Figure 11.1 indicates a simple wireless LAN configuration that is typical of many environments. There is a backbone wired LAN, such as Ethernet, that supports servers, workstations, and one or more bridges or routers to link with other networks. In addition, there is a control module (CM) that acts as an interface to a wireless LAN. The control module includes either bridge or router functionality to link the wireless LAN to the backbone. It includes some sort of access control logic, such as a polling or token-passing scheme, to regulate the access from the end systems. Note that some of the end systems are stand-alone devices, such as a workstation or a server. Hubs or other user modules (UMs) that control a number of stations off a wired LAN may also be part of the wireless LAN configuration.

The configuration of Figure 11.1 can be referred to as a single-cell wireless LAN; all of the wireless end systems are within the range of a single control module. This may be true of a small office or a home. Another common configuration, suggested by Figure 11.2, is a multiple-cell wireless LAN. In this case, there are multiple control modules interconnected by a wired LAN. Each control module supports a number of wireless end systems within its transmission range. For example, with IEEE 802.11ad WLAN, transmission is limited to a single room due to its use of 60 GHz frequencies; therefore, one cell is needed for each room in an office building that requires wireless support.

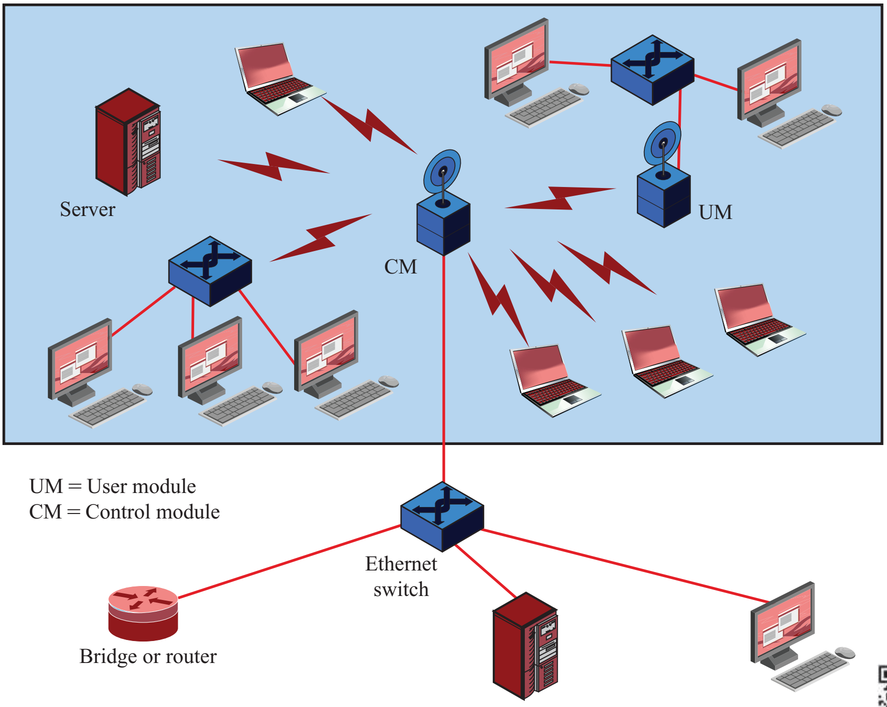


Figure 11.1 Example of Single-Cell Wireless LAN Configuration

An **ad hoc network** is a peer-to-peer network (no centralized server) set up temporarily to meet some immediate need. For example, a group of devices in a home may connect to share multimedia content. This may be a temporary network just for the duration of the multimedia session. Figure 11.3 shows a wireless LAN configured as an ad hoc wireless LAN. A peer collection of stations within the range of each other may dynamically configure themselves into a temporary network. WLANs can provide a wireless connectivity for an ad hoc network, as may Bluetooth, ZigBee, and other technologies mentioned in Chapter 12, depending on range, throughput, and power requirements.

Motivation

WLANs are providing many important capabilities. As newer standards exceed gigabit per second throughput, the following capabilities are enhanced [VERM13]:

- **Cellular data offloading:** The spectrum available in mobile cellular networks is limited and costly to consumers. Mobile devices such as smartphones, laptops, and tablets can use higher capacity WLANs. This is especially helpful in high density locations such as shopping malls, enterprises, universities, and even sporting venues.
- **Sync/file transfer:** Multi-gigabit Wi-Fi (Wireless Fidelity) allows synchronization between devices 10 times faster than previous Wi-Fi. For example, this eliminates the need to use cables to synchronize mobile devices.

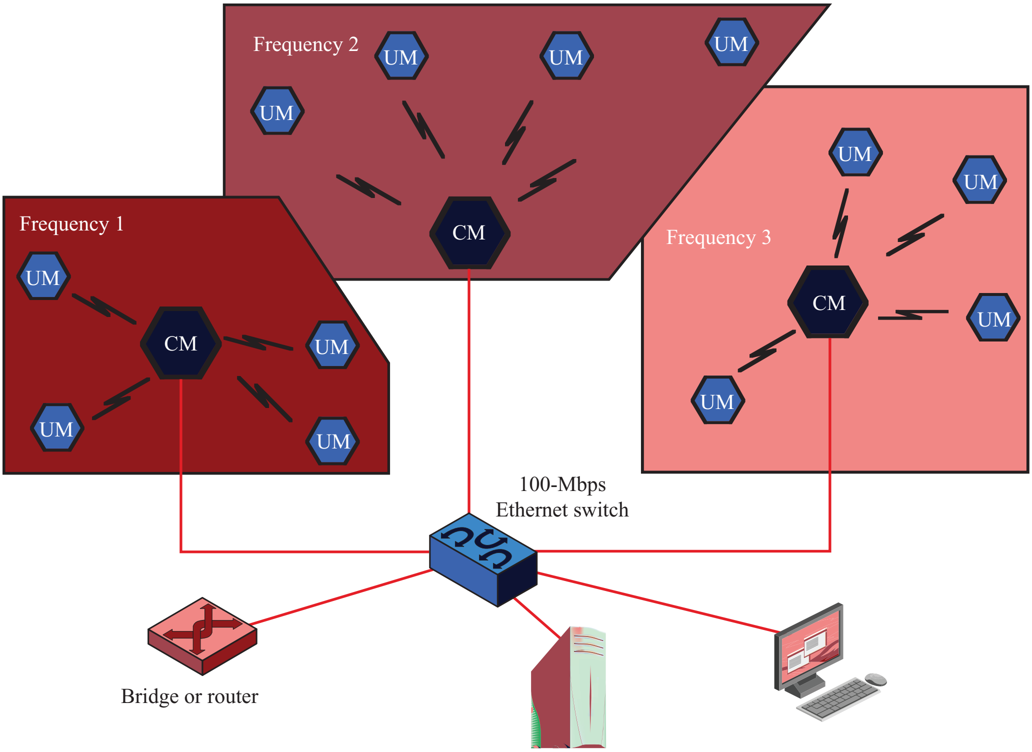


Figure 11.2 Example of Multiple-Cell Wireless LAN Configuration

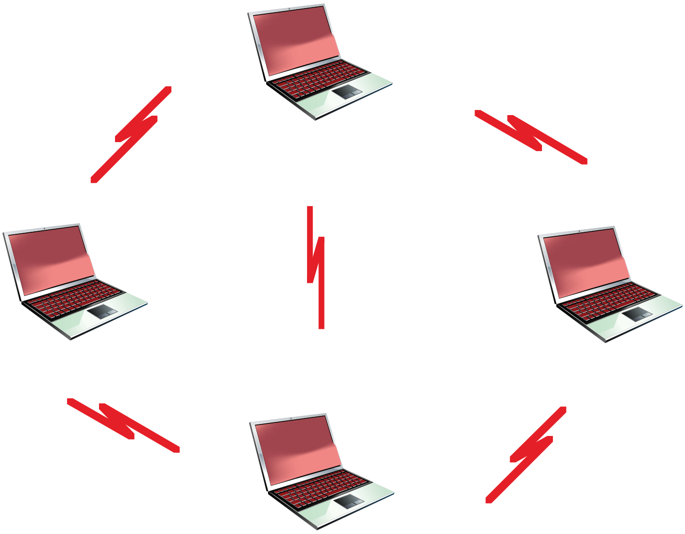


Figure 11.3 Ad Hoc Wireless LAN Configuration

- **Internet Access:** Multi-gigabit Wi-Fi enables faster Internet access, eliminating any significant bottlenecks from the WLAN.
- **Multimedia Streaming:** Streaming uncompressed video can require 3 Gbps, and streaming of compressed video has issues of quality and latency. Wi-Fi can be more suitable than other proposed wireless approaches because of its larger deployment, user awareness, support for IP networking, ease of connection, and standardized security mechanism.

Wireless LAN Requirements

A WLAN must meet the same sort of requirements typical of any LAN, including high capacity, ability to cover short distances, full connectivity among attached stations, and broadcast capability. In addition, there are a number of requirements specific to the wireless LAN environment. The following are among the most important requirements for wireless LANs:

- **Throughput:** The medium access control (MAC) protocol should make as efficient use as possible of the wireless medium to maximize capacity.
- **Number of nodes:** WLANs may need to support hundreds of nodes across multiple cells.
- **Connection to backbone LAN:** In most cases, interconnection with stations on a wired backbone LAN is required. For infrastructure WLANs, this is easily accomplished through the use of control modules that connect to both types of LANs. There may also need to be accommodation for mobile users with ad hoc wireless networks.
- **Service area:** A typical coverage area for a WLAN has a diameter of 100 to 300 m.
- **Battery power consumption:** Mobile workers use battery-powered smartphones, tablets, and workstations that need to have a long battery life. This suggests that a MAC protocol that requires mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station is inappropriate. Typical WLAN implementations have features to reduce power consumption, such as sleep modes, while not using the network.
- **Transmission robustness and security:** Unless properly designed, a WLAN may be especially vulnerable to interference and network eavesdropping. The design of a WLAN must permit reliable transmission even in a noisy environment and should provide security from eavesdropping.
- **Collocated network operation:** It is common for two or more wireless LANs to operate in the same area or in some area where interference between the WLANs is possible. Such interference may thwart the normal operation of a MAC algorithm and may allow unauthorized access to a particular WLAN.
- **License-free operation:** Users need to buy and operate WLAN products without having to secure a license for the frequency band used by the WLAN.
- **Handoff/roaming:** The MAC protocol used in the WLAN should enable mobile stations to move from one cell to another.

- **Dynamic configuration:** The MAC addressing and network management aspects of the WLAN should permit dynamic and automated addition, deletion, and relocation of end systems without disruption to other users.

It is instructive to compare wireless LANs to wired LANs and mobile data networks using **Kiviat graphs**,[1] as shown in Figure 11.4.

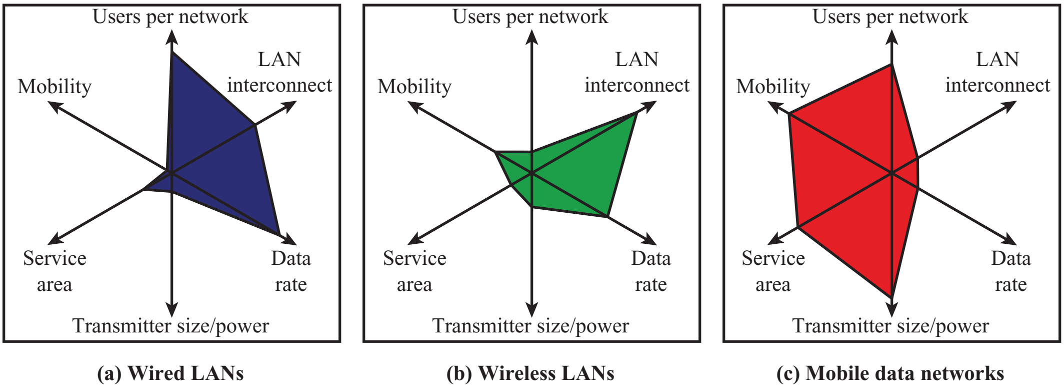
Wireless LAN Physical Layer

Wireless LANs use unlicensed spectrum. These use spread spectrum and orthogonal frequency division multiplexing (OFDM) techniques that must meet the regulatory requirements for those bands that are shared by many users and uses.

Configuration Except for quite small offices, a wireless LAN makes use of a multiple-cell arrangement, as illustrated in Figure 11.2. Adjacent cells make use of different center frequencies within the same band to avoid interference.

Within a given cell, the topology can be either hub or peer to peer. The hub topology is indicated in Figure 11.2. In a hub topology, the hub is typically mounted on the ceiling and connected to a backbone wired LAN to provide connectivity to stations attached to the wired LAN and to stations that are part of wireless LANs in other cells. The hub may also control access, as in the IEEE 802.11 point coordination function. The hub may also control access by acting as a multiport repeater with similar functionality to the multiport Ethernet repeaters. In this case, all stations in the cell transmit only to the hub and receive only from the hub. Alternatively, and regardless of access control mechanism, each station may broadcast using an omnidirectional antenna so that all other stations in the cell may receive; this corresponds to a logical bus configuration.

One other potential function of a hub is automatic handoff of mobile stations. At any time, a number of stations are dynamically assigned to a given hub based on



(a) Wired LANs **(b) Wireless LANs** **(c) Mobile data networks**

Figure 11.4 Kiviat Graphs for Data Networks

[1] A Kiviat graph provides a pictorial means of comparing systems along multiple variables. The variables are laid out at equal angular intervals. A given system is defined by one point on each variable; these points are connected to yield a shape that is characteristic of that system.

proximity. When the hub senses a weakening signal, it can automatically hand off to the nearest adjacent hub.

A peer-to-peer topology is one in which there is no hub. A MAC algorithm such as carrier sense multiple access (CSMA) is used to control access. This topology is appropriate for ad hoc LANs.

Transmission Issues A necessary characteristic of a wireless LAN is that it be usable without having to go through a licensing procedure. The licensing regulations differ from one country to another, which complicates this objective. Within the United States, the Federal Communications Commission (FCC) has authorized two unlicensed applications within the ISM (industrial, scientific, and medical) band: spread spectrum systems, which can operate at up to 1 watt, and very low power systems, which can operate at up to 0.5 watts. Since the FCC opened up this band, its use for spread spectrum wireless LANs became popular.

In the United States, there are four microwave bands of interest to us that have been set aside for unlicensed spread spectrum use: 902–928 MHz (915 MHz band), 2.4–2.5 GHz (2.4 GHz band), 5.725–5.875 GHz (5.8 GHz band), and 58-64 GHz (60 GHz band). Of these, the 2.4 GHz is also used in this manner in Europe and Japan. The higher the frequency, the higher the potential bandwidth, so the bands are of increasing order of attractiveness from a capacity point of view. In addition, the potential for interference must be considered. There are a number of devices that operate at around 900 MHz, including cordless telephones, wireless microphones, and amateur radio. There are fewer devices operating at 2.4 GHz; one notable example is the microwave oven, which tends to have greater leakage of radiation with increasing age. At present there is less competition at the 5.8 and 60 GHz bands; however, the higher the frequency band, in general, the more expensive the equipment.

Spread spectrum wireless LANs operate using either direct sequence spread spectrum (DSSS) or OFDM. Recent advances using OFDM, along with channel bonding and multiuser multiple-input-multiple-output (MIMO), have increased channel rates to well over 1 Gbps.

11.2 IEEE 802 ARCHITECTURE

The IEEE 802.11 working group developed the most prominent specification for WLANs. We look first at the overall architecture of IEEE 802 standards and then at the specifics of IEEE 802.11.

The architecture of a LAN is best described in terms of a layering of protocols that organize the basic functions of a LAN. This section opens with a description of the standardized protocol architecture for LANs, which encompasses physical, medium access control, and logical link control (LLC) layers. We then look in more detail at medium access control and logical link control.

Protocol Architecture

Protocols defined specifically for LAN and MAN (metropolitan area network) transmission address issues relating to the transmission of blocks of data over the network. In OSI terms (see Chapter 4), higher-layer protocols (layer 3 or 4 and above) are independent of network architecture and are applicable to LANs, MANs, and WANs. Thus, a discussion of LAN protocols is concerned principally with lower layers of the OSI model.

Figure 11.5 relates the LAN protocols to the OSI architecture(Figure 4.3). This architecture was developed by the IEEE 802 committee and has been adopted by all organizations working on the specification of LAN standards. It is generally referred to as the IEEE 802 reference model.[2]

Working from the bottom up, the lowest layer of the IEEE 802 reference model corresponds to the ***physical layer*** of the OSI model and includes such functions as

- Encoding/decoding of signals (e.g., PSK, QAM, etc.)
- Preamble generation/removal (for synchronization)
- Bit transmission/reception

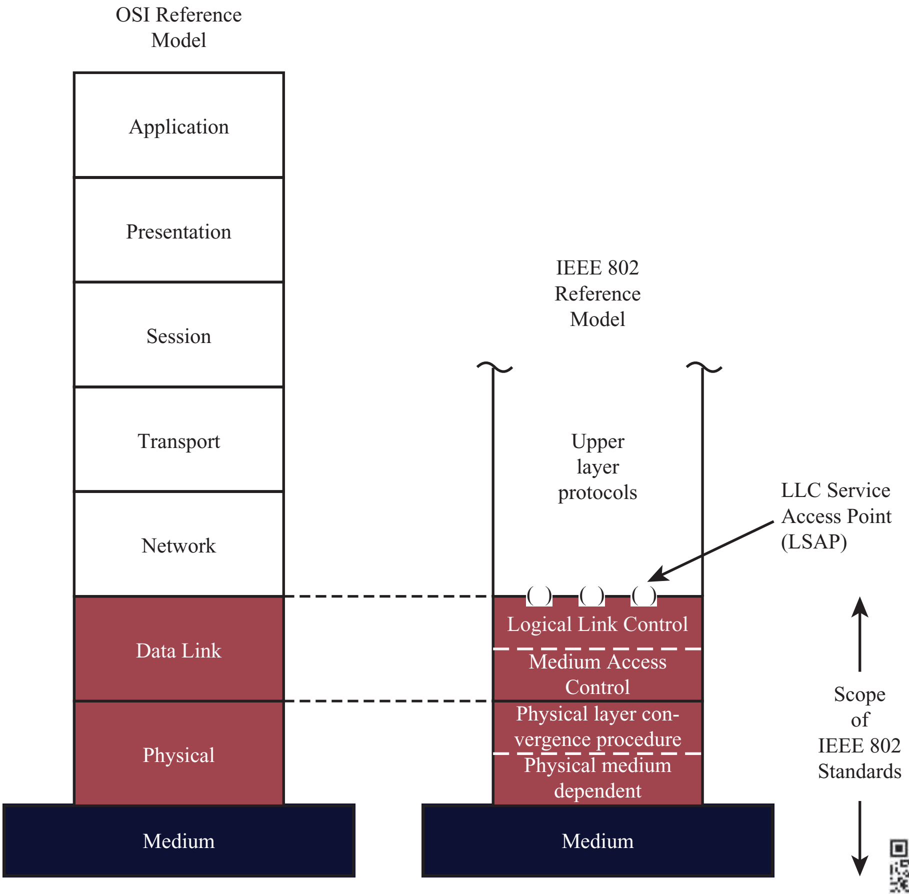


Figure 11.5 IEEE 802 Protocol Layers Compared to OSI Model

[2] A supporting document at this book's Web site provides an overview of the key organizations involved in developing communication and protocol standards, including the IEEE 802 Standards Committee.

In addition, the physical layer of the 802 model includes a specification of the transmission medium and the topology. Generally, this is considered "below" the lowest layer of the OSI model. However, the choice of transmission medium and topology is critical in LAN design, and so a specification of the medium is included. For some of the IEEE 802 standards, the physical layer is further subdivided into sublayers. In the case of IEEE 802.11, two sublayers are defined:

- **Physical layer convergence procedure (PLCP):** Defines a method of mapping 802.11 MAC layer protocol data units (MPDUs) into a framing format suitable for sending and receiving user data and management information between two or more stations using the associated PMD sublayer.
- **Physical medium dependent (PMD) sublayer:** Defines the characteristics of, and method of transmitting and receiving, user data through a wireless medium between two or more stations.

Above the physical layer are the functions associated with providing service to LAN users. These include

- On transmission, assemble data into a frame with address and error detection fields.
- On reception, disassemble frame and perform address recognition and error detection.
- Govern access to the LAN transmission medium.
- Provide an interface to higher layers and perform flow and error control.

These are functions typically associated with OSI layer 2. The set of functions in the last bullet item is grouped into a **logical link control (LLC)** layer. The functions in the first three bullet items are treated as a separate layer, called **medium access control (MAC)**. The separation is done for the following reasons:

- The logic required to manage access to a shared-access medium is not found in traditional layer 2 data link control.
- For the same LLC, several MAC options may be provided.

Figure 11.6 illustrates the relationship between the levels of the architecture. Higher-level data are passed down to LLC, which appends control information as a header, creating an ***LLC protocol data unit (PDU)***. This control information is used in the operation of the LLC protocol. The entire LLC PDU is then passed down to the MAC layer, which appends control information at the front and back of the packet, forming a ***MAC frame***. Again, the control information in the frame is needed for the operation of the MAC protocol. For context, the figure also shows the use of TCP/IP and an application layer above the LAN protocols.

MAC Frame Format

The MAC layer receives a block of data from the LLC layer and is responsible for performing functions related to medium access and for transmitting the data. As with other protocol layers, MAC implements these functions making use of a protocol data unit at its layer. In this case, the PDU is referred to as a MAC frame.

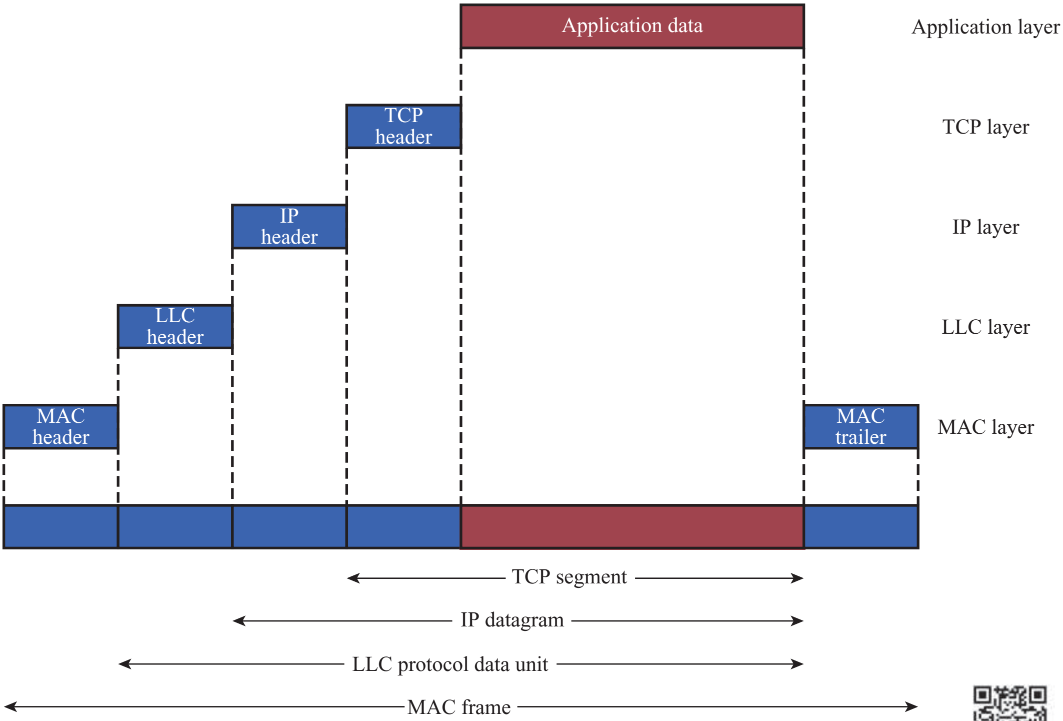


Figure 11.6 IEEE 802 Protocols in Context

The exact format of the MAC frame differs somewhat for the various MAC protocols in use. In general, all of the MAC frames have a format similar to that of Figure 11.7. The fields of this frame are as follows:

- **MAC:** This field contains any protocol control information needed for the functioning of the MAC protocol. For example, a priority level could be indicated here.
- **Destination MAC Address:** The destination physical attachment point on the LAN for this frame.
- **Source MAC Address:** The source physical attachment point on the LAN for this frame.
- **Data:** The body of the MAC frame. This may be LLC data from the next higher layer or control information relevant to the operation of the MAC protocol.
- **CRC:** The cyclic redundancy check field (also known as the frame check sequence, FCS, field). This is an error-detecting code, as described in Section 10.1. The CRC is used in virtually all data link protocols, such as high-level data link control (HDLC) (online Appendix C).

In most data link control protocols, the data link protocol entity is responsible not only for detecting errors using the CRC but for recovering from those errors by retransmitting damaged frames. In the LAN protocol architecture, these two functions are split between the MAC and LLC layers. The MAC layer is responsible for

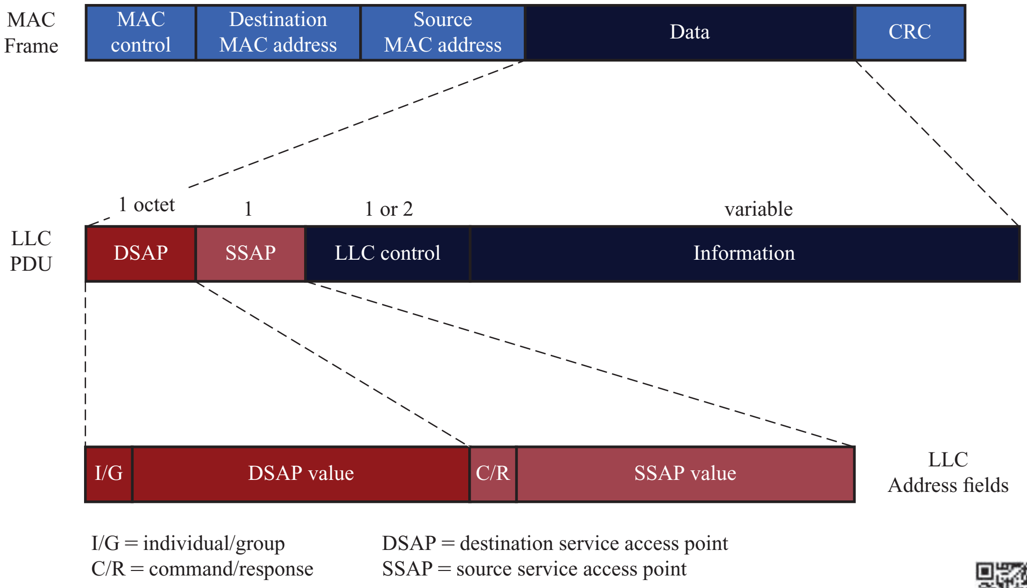


Figure 11.7 LLC PDU in a Generic MAC Frame Format

detecting errors and discarding any frames that are in error. The LLC layer optionally keeps track of which frames have been successfully received and retransmits unsuccessful frames.

Logical Link Control

The LLC layer for LANs is similar in many respects to other link layers in common use. Like all link layers, LLC is concerned with the transmission of a link-level PDU between two stations, without the necessity of an intermediate switching node. LLC has two characteristics not shared by most other link control protocols:

1. It must support the multiaccess, shared-medium nature of the link (this differs from a multidrop line in that there is no primary node).
2. It is relieved of some details of link access by the MAC layer.

Addressing in LLC involves specifying the source and destination LLC users. Typically, a user is a higher-layer protocol or a network management function in the station. These LLC user addresses are referred to as service access points (SAPs), in keeping with OSI terminology for the user of a protocol layer.

We look first at the services that LLC provides to a higher-level user, and then at the LLC protocol.

LLC Services LLC specifies the mechanisms for addressing stations across the medium and for controlling the exchange of data between two users. The operation and format of this standard is based on HDLC. LLC provides three alternative services for attached devices:

- **Unacknowledged connectionless service:** This is a datagram-style service. It is a very simple service that does not involve any flow- and error-control mechanisms. Thus, the delivery of data is not guaranteed. However, in most devices, there will be some higher layer of software that deals with reliability issues.

- **Connection-mode service:** This service is similar to that offered by HDLC. A logical connection is set up between two users exchanging data, and flow control and error control are provided.
- **Acknowledged connectionless service:** This is a cross between the previous two services. It provides that datagrams are to be acknowledged, but no prior logical connection is set up.

Typically, a vendor will provide these services as options that the customer can select when purchasing the equipment. Alternatively, the customer can purchase equipment that provides two or all three services and select a specific service based on application.

The ***unacknowledged connectionless service*** requires minimum logic and is useful in two contexts. First, it will often be the case that higher layers of software will provide the necessary reliability and flow-control mechanism, and it is efficient to avoid duplicating them. For example, TCP could provide the mechanisms needed to ensure that data are delivered reliably. Second, there are instances in which the overhead of connection establishment and maintenance is unjustified or even counterproductive (for example, data collection activities that involve the periodic sampling of data sources, such as sensors and automatic self-test reports from security equipment or network components). In a monitoring application, the loss of an occasional data unit would not cause distress, as the next report should arrive shortly. Thus, in most cases, the unacknowledged connectionless service is the preferred option.

The ***connection-mode service*** could be used in very simple devices, such as remote sensors, that have little software operating above this level. In these cases, it would provide the flow control and reliability mechanisms normally implemented at higher layers of the communications software.

The ***acknowledged connectionless service*** is useful in several contexts. With the connection-mode service, the logical link control software must maintain some sort of table for each active connection, to keep track of the status of that connection. If the user needs guaranteed delivery but there are a large number of destinations for data, then the connection-mode service may be impractical because of the large number of tables required. An example is a process control or automated factory environment where a central site may need to communicate with a large number of processors and programmable controllers. Another use of this is the handling of important and time-critical alarm or emergency control signals in a factory. Because of their importance, an acknowledgment is needed so that the sender can be assured that the signal got through. Because of the urgency of the signal, the user might not want to take the time first to establish a logical connection and then send the data.

LLC Protocol

The basic LLC protocol is modeled after HDLC and has similar functions and formats. The differences between the two protocols can be summarized as follows:

- LLC makes use of the asynchronous balanced mode of operation of HDLC, to support connection-mode LLC service; this is referred to as type 2 operation. The other HDLC modes are not employed.
- LLC supports an unacknowledged connectionless service using the unnumbered information PDU; this is known as type 1 operation.
- LLC supports an acknowledged connectionless service by using two new unnumbered PDUs; this is known as type 3 operation.
- LLC permits multiplexing by the use of LLC service access points (LSAPs).

All three LLC protocols employ the same PDU format (Figure 11.7), which consists of four fields. The destination service access point (DSAP) and source service access point (SSAP) fields each contain a 7-bit address, which specify the destination and source users of LLC, respectively. One bit of the DSAP indicates whether the DSAP is an individual or group address. One bit of the SSAP indicates whether the PDU is a command or response PDU. The format of the LLC control field is identical to that of HDLC, using extended (7-bit) sequence numbers.

For ***type 1 operation***, which supports the unacknowledged connectionless service, the unnumbered information (UI) PDU is used to transfer user data. There is no acknowledgment, flow control, or error control. However, there is error detection and discard at the MAC level.

Two other PDU types, XID and TEST, are used to support management functions associated with all three types of operation. Both PDU types are used in the following fashion. An LLC entity may issue a command (C/R bit = 0) XID or TEST. The receiving LLC entity issues a corresponding XID or TEST in response. The XID PDU is used to exchange two types of information: types of operation supported and window size. The TEST PDU is used to conduct a loopback test of the transmission path between two LLC entities. Upon receipt of a TEST command PDU, the addressed LLC entity issues a TEST response PDU as soon as possible.

With ***type 2 operation***, a data link connection is established between two LLC SAPs prior to data exchange. Connection establishment is attempted by the type 2 protocol in response to a request from a user. The LLC entity issues a SABME PDU[3] to request a logical connection with the other LLC entity. If the connection is accepted by the LLC user designated by the DSAP, then the destination LLC entity returns an unnumbered acknowledgment (UA) PDU. The connection is henceforth uniquely identified by the pair of user SAPs. If the destination LLC user rejects the connection request, its LLC entity returns a disconnected mode (DM) PDU.

Once the connection is established, data are exchanged using information PDUs, as in HDLC. Information PDUs include send and receive sequence numbers, for sequencing and flow control. The supervisory PDUs are used, as in HDLC,

[3] This stands for *set asynchronous balanced mode extended*. It is used in HDLC to choose ABM and to select extended sequence numbers of 7 bits. Both ABM and 7-bit sequence numbers are mandatory in type 2 operation.

for flow control and error control. Either LLC entity can terminate a logical LLC connection by issuing a disconnect (DISC) PDU.

With ***type 3 operation***, each transmitted PDU is acknowledged. A new (not found in HDLC) unnumbered PDU, the acknowledged connectionless (AC) information PDU, is defined. User data are sent in AC command PDUs and must be acknowledged using an AC response PDU. To guard against lost PDUs, a 1-bit sequence number is used. The sender alternates the use of 0 and 1 in its AC command PDU, and the receiver responds with an AC PDU with the opposite number of the corresponding command. Only one PDU in each direction may be outstanding at any time.

11.3 IEEE 802.11 ARCHITECTURE AND SERVICES

In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, specifically devoted to WLANs, with a charter to develop a MAC protocol and physical medium specification. The initial interest was in developing a WLAN operating in the ISM band. Since that time, the demand for WLANs, at different frequencies and data rates, has exploded. Keeping pace with this demand, the IEEE 802.11 working group has issued an ever-expanding list of standards (Table 11.1). Table 11.2 briefly defines key terms used in the IEEE 802.11 standard.

Table 11.1 IEEE 802.11 Standards

Standard	Date	Scope
IEEE 802.11	1997	Medium access control (MAC): One common MAC for WLAN applications
		Physical layer: Infrared at 1 and 2 Mbps
		Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
		Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	1999	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	1999	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	2003	Bridge operation at 802.11 MAC layer
IEEE 802.11d	2001	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	2007	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	2003	Recommended practices for multivendor access point interoperability
IEEE 802.11g	2003	Physical layer: Extend 802.11b to data rates $>$20 Mbps
IEEE 802.11h	2003	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management

Standard	Date	Scope
IEEE 802.11i	2007	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	2007	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	2008	Radio Resource Measurement enhancements to provide interface to higher layers for radio and network measurements
IEEE 802.11m	Ongoing	This group provides maintenance of the IEEE 802.11 standard by rolling published amendments into revisions of the 802.11 standard.
IEEE 802.11n	2009	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	2010	Wireless Access in Vehicular Environments (WAVE)
IEEE 802.11r	2008	Fast Roaming/Fast BSS Transition
IEEE 802.11s	2011	Mesh Networking
IEEE 802.11T	Abandoned	Recommended Practice for Evaluation of 802.11 Wireless Performance
IEEE 802.11u	2011	Interworking with External Networks
IEEE 802.11v	2011	Wireless Network Management
IEEE 802.11w	2009	Protected Management Frames
IEEE 802.11y	2008	Contention Based Protocol
IEEE 802.11z	2010	Extensions to Direct Link Setup
IEEE 802.11aa	2012	Video Transport Stream
IEEE 802.11ac	Ongoing	Very High Throughput <6 GHz
IEEE 802.11ad	2012	Very High Throughput in 60 GHz
IEEE 802.11ae	2012	Prioritization of Management Frames
IEEE 802.11af	Ongoing	Wireless LAN in the TV White Space
IEEE 802.11ah	Ongoing	Sub 1 GHz
IEEE 802.11ai	Ongoing	Fast Initial Link Setup
IEEE 802.11aj	Ongoing	China Milli-Meter Wave (CMMW)
IEEE 802.11ak	Ongoing	Enhancements For Transit Links Within Bridged Networks
IEEE 802.11aq	Ongoing	Pre-Association Discovery (PAD)
IEEE 802.11ax	Ongoing	High Efficiency WLAN (HEW)

The Wi-Fi Alliance

Although 802.11 products are all based on the same standards, there is always a concern whether products from different vendors will successfully interoperate. To meet this concern, the Wireless Ethernet Compatibility Alliance (WECA), an industry consortium, was formed in 1999. This organization, subsequently renamed the Wi-Fi Alliance, created a test suite to certify interoperability for 802.11b products. The term used for certified 802.11b products is **Wi-Fi**. Wi-Fi certification has been extended to other 802.11 products.

The Wi-Fi Alliance is concerned with a range of market areas for WLANs, including enterprise, home, and hot spots.

Table 11.2 IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

IEEE 802.11 Architecture

Figure 11.8 illustrates the model developed by the 802.11 working group. The smallest building block of a WLAN is a **basic service set (BSS)**, which consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium. A BSS may be isolated or it may connect to a backbone **distribution system (DS)** through an **access point (AP)**. The AP functions as a bridge and a relay point. In a BSS, client stations do not communicate directly with one another. Rather, if one station in the BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from the originating station to the AP, and then from the AP to the destination station. Similarly, a MAC frame from a station in the BSS to a remote station is sent from the local station to the AP and then relayed by the AP over the DS on its way to the destination station. The BSS generally corresponds to what is referred to as a cell in the literature. The DS can be a switch, a wired network, or a wireless network.

When all the stations in the BSS are mobile stations, with no connection to other BSSs, the BSS is called an **independent BSS (IBSS)**. An IBSS is typically an ad hoc network. In an IBSS, the stations all communicate directly, and no AP is involved.

A simple configuration is shown in Figure 11.8, in which each station belongs to a single BSS; that is, each station is within wireless range only of other stations within the same BSS. It is also possible for two BSSs to overlap geographically, so that a single station could participate in more than one BSS. Further, the association between a station and a BSS is dynamic. Stations may turn off, come within range, and go out of range.

An **extended service set (ESS)** consists of two or more BSSs interconnected by a distribution system. Typically, the distribution system is a wired backbone LAN but can be any communications network. The ESS appears as a single logical LAN to the LLC level.

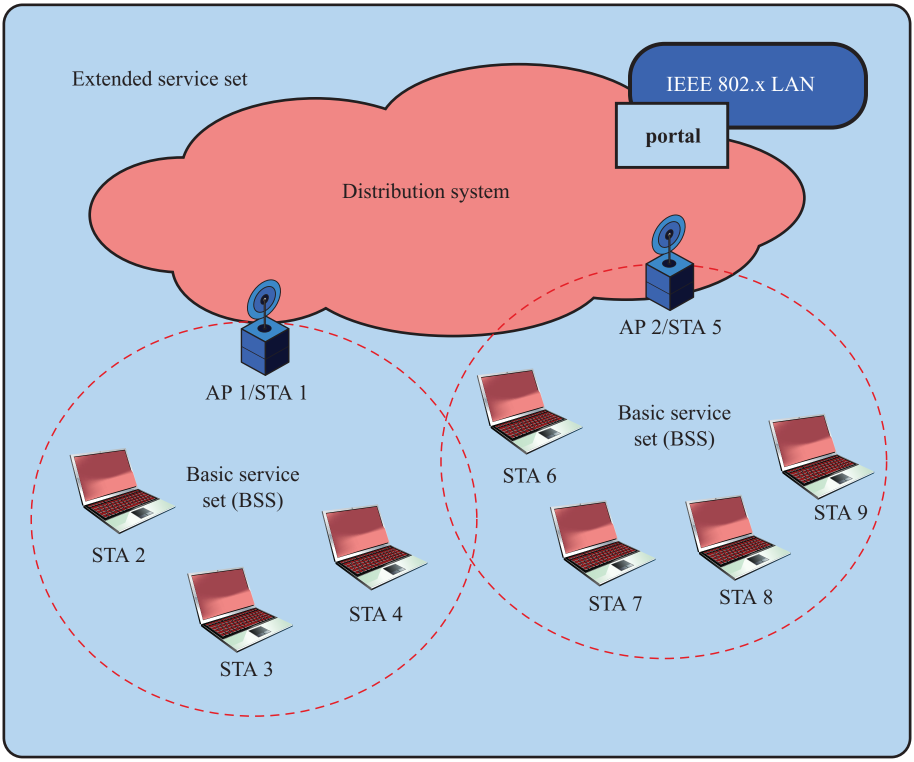


Figure 11.8 IEEE 802.11 Extended Service Set

Figure 11.8 indicates that an AP is implemented as part of a station; the AP is the logic within a station that provides access to the DS by providing DS services in addition to acting as a station. To integrate the IEEE 802.11 architecture with a traditional wired LAN, a ***portal*** is used. The portal logic is implemented in a device, such as a bridge or router, that is part of the wired LAN and that is attached to the DS.

IEEE 802.11 Services

IEEE 802.11 defines nine services that need to be provided by the wireless LAN to provide functionality equivalent to that which is inherent to wired LANs. Table 11.3 lists the services and indicates two ways of categorizing them.

1. The service provider can be either the station or the DS. Station services are implemented in every 802.11 station, including AP stations. Distribution services are provided between BSSs; these services may be implemented in an AP or in another special-purpose device attached to the distribution system.
2. Three of the services are used to control IEEE 802.11 LAN access and confidentiality. Six of the services are used to support delivery of **MAC service data units (MSDUs)** between stations. The MSDU is the block of data passed down from the MAC user to the MAC layer; typically this is an LLC PDU.

Table 11.3 IEEE 802.11 Services

Service	Provider	Used to Support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

> If the MSDU is too large to be transmitted in a single MAC frame, it may be fragmented and transmitted in a series of MAC frames. Fragmentation is discussed in Section 11.4.

Following the IEEE 802.11 document, we next discuss the services in an order designed to clarify the operation of an IEEE 802.11 ESS network. MSDU delivery, which is the basic service, has already been mentioned. Services related to security are discussed in Section 11.8.

Distribution of Messages within a DS The two services involved with the distribution of messages within a DS are distribution and integration. ***Distribution*** is the primary service used by stations to exchange MAC frames when the frame must traverse the DS to get from a station in one BSS to a station in another BSS. For example, suppose a frame is to be sent from station 2 (STA 2) to STA 7 in Figure 11.8. The frame is sent from STA 2 to STA 1, which is the AP for this BSS. The AP gives the frame to the DS, which has the job of directing the frame to the AP associated with STA 5 in the target BSS. STA 5 receives the frame and forwards it to STA 7. How the message is transported through the DS is beyond the scope of the IEEE 802.11 standard.

If the two stations that are communicating are within the same BSS, then the distribution service logically goes through the single AP of that BSS.

The ***integration*** service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN. The term *integrated* refers to a wired LAN that is physically connected to the DS and whose stations may be logically connected to an IEEE 802.11 LAN via the integration service. The integration service takes care of any address translation and media conversion logic required for the exchange of data.

Association-Related Services The primary purpose of the MAC layer is to transfer MSDUs between MAC entities; this purpose is fulfilled by the distribution service. For that service to function, it requires information about stations within the ESS, which is provided by the association-related services. Before the distribution service can deliver data to or accept data from a station, that station must be *associated*.

Before looking at the concept of association, we need to describe the concept of mobility. The standard defines three transition types, based on mobility:

- **No transition:** A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.
- **BSS transition:** This is defined as a station movement from one BSS to another BSS within the same ESS. In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.
- **ESS transition:** This is defined as a station movement from a BSS in one ESS to a BSS within another ESS. This case is supported only in the sense that the station can move. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed. In fact, disruption of service is likely to occur.

To deliver a message within a DS, the distribution service needs to know where the destination station is located. Specifically, the DS needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station. To meet this requirement, a station must maintain an association with the AP within its current BSS. Three services relate to this requirement:

- **Association:** Establishes an initial association between a station and an AP. Before a station can transmit or receive frames on a WLAN, its identity and address must be known. For this purpose, a station must establish an association with an AP within a particular BSS. The AP can then communicate this information to other APs within the ESS to facilitate routing and delivery of addressed frames.
- **Reassociation:** Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
- **Disassociation:** A notification from either a station or an AP that an existing association is terminated. A station should give this notification before leaving an ESS or shutting down. However, the MAC management facility protects itself against stations that disappear without notification.

11.4 IEEE 802.11 MEDIUM ACCESS CONTROL

The IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, access control, and security. This section covers the first two topics and Section 11.8 covers the third.

Reliable Data Delivery

As with any wireless network, a WLAN using the IEEE 802.11 physical and MAC layers is subject to considerable unreliability. Noise, interference, and other propagation effects result in the loss of a significant number of frames. Even with error-correction codes, a number of MAC frames may not successfully be received. This situation can be dealt with by reliability mechanisms at a higher layer, such as TCP. However, timers used for retransmission at higher layers are typically on the order of seconds. It is therefore more efficient to deal with errors at the MAC level. For this purpose, IEEE 802.11 includes a frame exchange protocol. When a station receives a data frame from another station, it returns an acknowledgment (ACK) frame to the source station. This exchange is treated as an atomic unit, not to be interrupted by a transmission from any other station. If the source does not receive an ACK within a short period of time, either because its data frame was damaged or because the returning ACK was damaged, the source retransmits the frame.

Thus, the basic data transfer mechanism in IEEE 802.11 involves an exchange of two frames. To further enhance reliability, a four-frame exchange may be used. In this scheme, a source first issues a request to send (RTS) frame to the destination. The destination then responds with a clear to send (CTS). After receiving the CTS, the source transmits the data frame, and the destination responds with an ACK. The RTS alerts all stations that are within reception range of the source that an exchange is under way; these stations refrain from transmission in order to avoid a collision between two frames transmitted at the same time. Similarly, the CTS alerts all stations that are within reception range of the destination that an exchange is under way. The RTS/CTS portion of the exchange is a required function of the MAC but may be disabled.

Medium Access Control

The 802.11 working group considered two types of proposals for a MAC algorithm: distributed access protocols, which, like Ethernet, distribute the decision to transmit over all the nodes using a carrier-sense mechanism; and centralized access protocols, which involve regulation of transmission by a centralized decision maker. A distributed access protocol makes sense for an ad hoc network of peer workstations (typically an IBSS) and may also be attractive in other WLAN configurations that consist primarily of bursty traffic. A centralized access protocol is natural for configurations in which a number of wireless stations are interconnected with each other and some sort of base station that attaches to a backbone wired LAN; it is especially useful if some of the data are time sensitive or high priority.

The end result for 802.11 is a MAC algorithm called DFWMAC (distributed foundation wireless MAC) that provides a distributed access control mechanism with an optional centralized control built on top of that. Figure 11.9 illustrates the architecture. The lower sublayer of the MAC layer is the **distributed coordination function (DCF)**. DCF uses a contention algorithm to provide access to all traffic. Ordinary asynchronous traffic directly uses DCF. The **point coordination function (PCF)** is a centralized MAC algorithm used to provide contention-free service. PCF is built on top of DCF and exploits features of DCF to assure access for its users. Let us consider these two sublayers in turn.

Distributed Coordination Function

The DCF sublayer makes use of a simple CSMA (carrier sense multiple access) algorithm. If a station has a MAC frame to transmit, it listens to the medium. If the medium is idle, the station may transmit; otherwise the station must wait until the current transmission is complete before

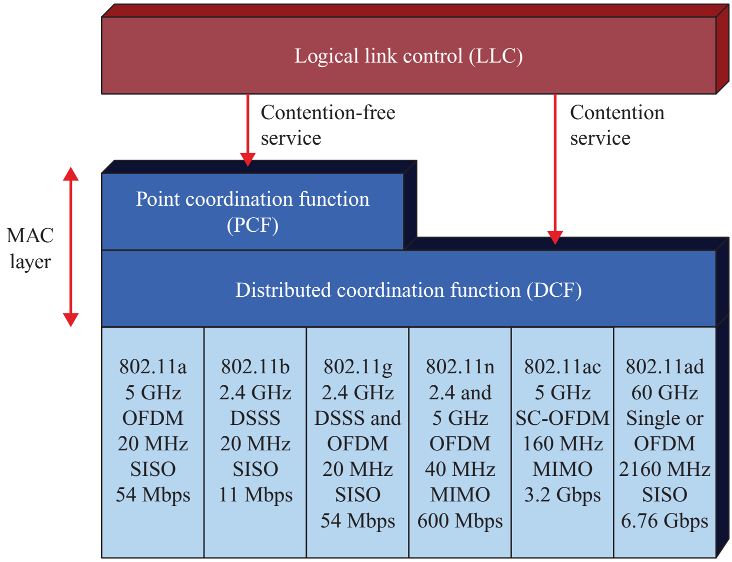

Logical link control (LLC)
Contention-free service
Contention service
MAC layer
Point coordination function (PCF)
Distributed coordination function (DCF)
802.11a 5 GHz OFDM 20 MHz SISO 54 Mbps
802.11b 2.4 GHz DSSS 20 MHz SISO 11 Mbps
802.11g 2.4 GHz DSSS and OFDM 20 MHz SISO 54 Mbps
802.11n 2.4 and 5 GHz OFDM 40 MHz MIMO 600 Mbps
802.11ac 5 GHz SC-OFDM 160 MHz MIMO 3.2 Gbps
802.11ad 60 GHz Single or OFDM 2160 MHz SISO 6.76 Gbps

Figure 11.9 IEEE 802.11 Protocol Architecture

transmitting. The DCF does not include a collision detection function (i.e., CSMA/CD) because collision detection is not practical on a wireless network. The dynamic range of the signals on the medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission.

To ensure the smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme. Let us start by considering a single delay known as an interframe space (IFS). In fact, there are three different IFS values, but the algorithm is best explained by initially ignoring this detail. Using an IFS, the rules for CSMA are as follows (Figure 11.10):

1. A station with a frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately.
2. If the medium is busy (either because the station initially finds the medium busy or because the medium becomes busy during the IFS idle time), the station defers transmission and continues to monitor the medium until the current transmission is over.
3. Once the current transmission is over, the station delays another IFS. If the medium remains idle for this period, then the station backs off a random amount of time and again senses the medium. If the medium is still idle, the station may transmit. During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle.
4. If the transmission is unsuccessful, which is determined by the absence of an acknowledgment, then it is assumed that a collision has occurred.

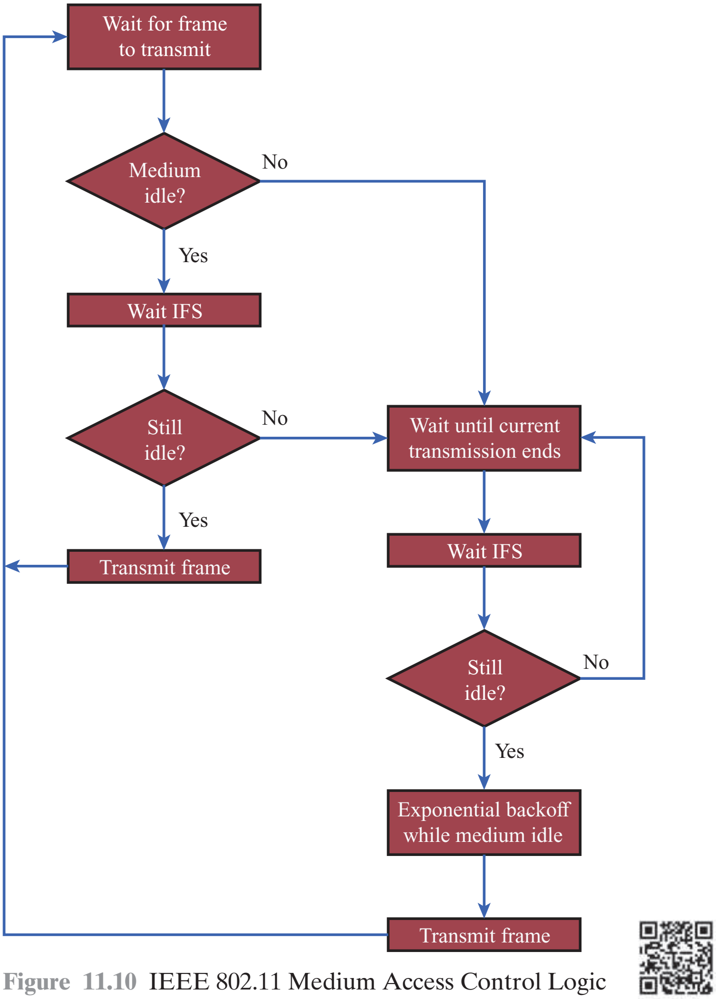

Wait for frame to transmit
Medium idle?
No
Yes
Wait IFS
Still idle?
No
Yes
Transmit frame
Wait until current transmission ends
Wait IFS
Still idle?
No
Yes
Exponential backoff while medium idle
Transmit frame

Figure 11.10 IEEE 802.11 Medium Access Control Logic

To ensure that backoff maintains stability, a technique known as **binary exponential backoff** is used. A station will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled up to some maximum value. The binary exponential backoff provides a means of handling a heavy load. Repeated failed attempts to transmit result in longer and longer backoff times, which helps to smooth out the load. Without such a backoff, the following situation could occur. Two or more stations attempt to transmit at the same time, causing a collision. These stations then immediately attempt to retransmit, causing a new collision.

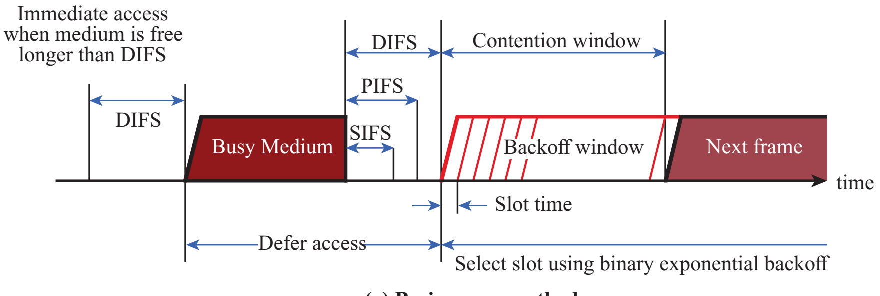
The preceding scheme is refined for DCF to provide priority-based access by the simple expedient of using three values for IFS:

- **SIFS (short IFS):** The shortest IFS, used for all immediate response actions, as explained in the following discussion.

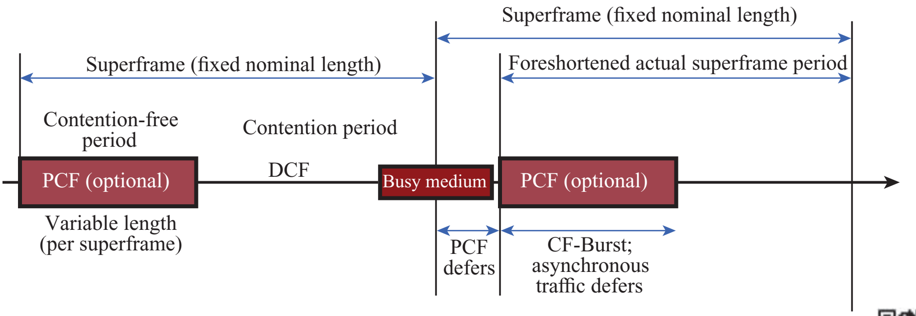
- **PIFS (point coordination function IFS):** A midlength IFS, used by the centralized controller in the PCF scheme when issuing polls.
- **DIFS (distributed coordination function IFS):** The longest IFS, used as a minimum delay for asynchronous frames contending for access.

Figure 11.11a illustrates the use of these time values. Consider first the SIFS. Any station using SIFS to determine transmission opportunity has, in effect, the highest priority, because it will always gain access in preference to a station waiting an amount of time equal to PIFS or DIFS. The SIFS is used in the following circumstances:

- **Acknowledgment (ACK):** When a station receives a frame addressed only to itself (not multicast or broadcast), it responds with an ACK frame after waiting only for an SIFS gap. This has two desirable effects. First, because collision detection is not used, the likelihood of collisions is greater than with CSMA/CD, and the MAC-level ACK provides for efficient collision recovery. Second, the SIFS can be used to provide efficient delivery of an LLC PDU that requires multiple MAC frames. In this case, the following scenario occurs. A station with a multiframe LLC PDU to transmit sends out the MAC frames one at a time. Each frame is acknowledged by the recipient after SIFS. When the source receives an ACK, it immediately (after SIFS) sends the next frame in the sequence. The result is that once a station has contended for the channel, it will maintain control of the channel until it has sent all of the fragments of an LLC PDU.



(a) Basic access method



(b) PCF superframe construction

Figure 11.11 IEEE 802.11 MAC Timing

- **Clear to send (CTS):** A station can ensure that its data frame will get through by first issuing a small RTS frame. The station to which this frame is addressed should immediately respond with a CTS frame if it is ready to receive. All other stations receive the RTS and defer using the medium.
- **Poll response:** This is explained in the following discussion of PCF.

The next longest IFS interval is the PIFS. This is used by the centralized controller in issuing polls and takes precedence over normal contention traffic. However, those frames transmitted using SIFS have precedence over a PCF poll.

Finally, the DIFS interval is used for all ordinary asynchronous traffic.

Point Coordination Function PCF is an alternative access method implemented on top of the DCF. The operation consists of polling by the centralized polling master (point coordinator). The point coordinator makes use of PIFS when issuing polls. Because PIFS is smaller than DIFS, the point coordinator can seize the medium and lock out all asynchronous traffic while it issues polls and receives responses.

As an extreme, consider the following possible scenario. A wireless network is configured so that a number of stations with time-sensitive traffic are controlled by the point coordinator while remaining traffic contends for access using CSMA. The point coordinator could issue polls in a round-robin fashion to all stations configured for polling. When a poll is issued, the polled station may respond using SIFS. If the point coordinator receives a response, it issues another poll using PIFS. If no response is received during the expected turnaround time, the coordinator issues a poll.

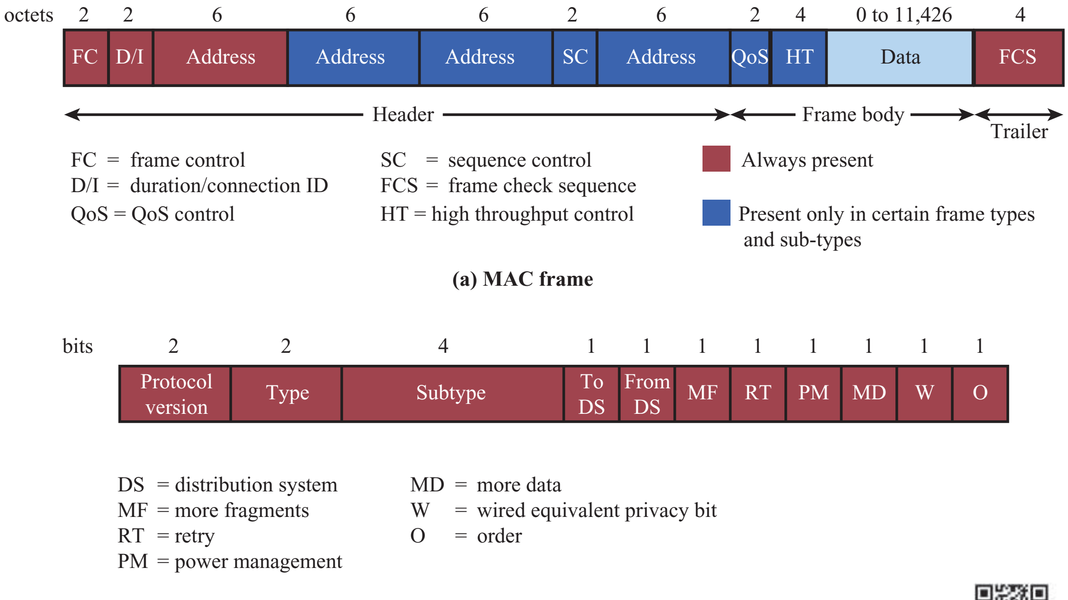
If the discipline of the preceding paragraph were implemented, the point coordinator would lock out all asynchronous traffic by repeatedly issuing polls. To prevent this, an interval known as the superframe is defined. During the first part of this interval, the point coordinator issues polls in a round-robin fashion to all stations configured for polling. The point coordinator then idles for the remainder of the superframe, allowing a contention period for asynchronous access.

Figure 11.11b illustrates the use of the superframe. At the beginning of a superframe, the point coordinator may optionally seize control and issue polls for a given period of time. This interval varies because of the variable frame size issued by responding stations. The remainder of the superframe is available for contention-based access. At the end of the superframe interval, the point coordinator contends for access to the medium using PIFS. If the medium is idle, the point coordinator gains immediate access and a full superframe period follows. However, the medium may be busy at the end of a superframe. In this case, the point coordinator must wait until the medium is idle to gain access; this results in a foreshortened superframe period for the next cycle.

MAC Frame

Figure 11.12a shows the format of 802.11, also known as the **MAC protocol data unit (MPDU)**. This general format is used for all data and control frames, but not all fields are used in all contexts. The fields are:

- **Frame Control:** Indicates the type of frame (control, management, or data) and provides control information. Control information includes whether the frame is to or from a DS, fragmentation information, and privacy information.



(a) MAC frame

(b) Frame control field

Figure 11.12 IEEE 802.11 MAC Frame Format

- **Duration/Connection ID:** If used as a duration field, indicates the time (in microseconds) the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection, identifier.
- **Addresses:** The number and meaning of the 48-bit address fields depend on context. The ***transmitter address*** and ***receiver address*** are the MAC addresses of stations joined to the BSS that are transmitting and receiving frames over the WLAN. The **service set identifier (SSID)** identifies the WLAN over which a frame is transmitted. For an IBSS, the SSID is a random number generated at the time the network is formed. For a wireless LAN that is part of a larger configuration, the SSID identifies the BSS over which the frame is transmitted; specifically, the SSID is the MAC-level address of the AP for this BSS (Figure 11.8). Finally the ***source address*** and ***destination address*** are the MAC addresses of stations, wireless or otherwise, that are the ultimate source and destination of this frame. The source address may be identical to the transmitter address and the destination address may be identical to the receiver address.
- **Sequence Control:** Contains a 4-bit fragment number subfield, used for fragmentation and reassembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.
- **QoS Control:** Contains information relating to the IEEE 802.11 quality of service (QoS) facility.
- **High Throughput Control:** This field contains control bits related to the operation of 802.11n, 802.11ac, and 802.11ad.
- **Frame Body:** Contains an MSDU or a fragment of an MSDU. The MSDU is a LLC protocol data unit or MAC control information.
- **Frame Check Sequence:** A 32-bit cyclic redundancy check.

The frame control field, shown in Figure 11.12b, consists of the following fields:

- **Protocol Version:** 802.11 version, currently version 0.
- **Type:** Identifies the frame as control, management, or data.
- **Subtype:** Further identifies the function of frame. Table 11.4 defines the valid combinations of type and subtype.
- **To DS:** The MAC coordination sets this bit to 1 in a frame destined to the distribution system.
- **From DS:** The MAC coordination sets this bit to 1 in a frame leaving the distribution system.
- **More Fragments:** Set to 1 if more fragments follow this one.
- **Retry:** Set to 1 if this is a retransmission of a previous frame.

Table 11.4 Valid Type and Subtype Combinations

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message
00	Management	1010	Dissociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
01	Control	1010	Power save-poll
01	Control	1011	Request to send
01	Control	1100	Clear to send
01	Control	1101	Acknowledgment
01	Control	1110	Contention-free (CF)-end
01	Control	1111	CF-end + CF-ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-poll (no data)
10	Data	0111	CF-Ack + CF-poll (no data)

- **Power Management:** Set to 1 if the transmitting station is in a sleep mode.
- **More Data:** Indicates that a station has additional data to send. Each block of data may be sent as one frame or a group of fragments in multiple frames.
- **WEP:** Set to 1 if the optional wired equivalent privacy is implemented. WEP is used in the exchange of encryption keys for secure data exchange. This bit also is set if the newer WPA security mechanism is employed, as described in Section 11.8.
- **Order:** Set to 1 in any data frame sent using the Strictly Ordered service, which tells the receiving station that frames must be processed in order.

We now look at the three MAC frame types.

Control Frames Control frames assist in the reliable delivery of data frames. There are six control frame subtypes:

- **Power Save-Poll (PS-Poll):** This frame is sent by any station to the station that includes the AP (access point). Its purpose is to request that the AP transmit a frame that has been buffered for this station while the station was in power-saving mode.
- **Request to Send:** This is the first frame in the four-way frame exchange discussed under the subsection on reliable data delivery at the beginning of Section 11.4. The station sending this message is alerting a potential destination, and all other stations within reception range, that it intends to send a data frame to that destination.
- **Clear to Send:** This is the second frame in the four-way exchange. It is sent by the destination station to the source station to grant permission to send a data frame.
- **Acknowledgment:** Provides an acknowledgment from the destination to the source that the immediately preceding data, management, or PS-Poll frame was received correctly.
- **Contention-Free (CF)-End:** Announces the end of a contention-free period that is part of the point coordination function.
- **CF-End + CF-Ack**: Acknowledges the CF-end. This frame ends the contention-free period and releases stations from the restrictions associated with that period.

Data Frames There are eight data frame subtypes, organized into two groups. The first four subtypes define frames that carry upper-level data from the source station to the destination station. The four data-carrying frames are as follows:

- **Data:** This is the simplest data frame. It may be used in both a contention period and a contention-free period.
- **Data + CF-Ack:** May only be sent during a contention-free period. In addition to carrying data, this frame acknowledges previously received data.
- **Data + CF-Poll:** Used by a point coordinator to deliver data to a mobile station and also to request that the mobile station send a data frame that it may have buffered.

- **Data + CF-Ack + CF-Poll:** Combines the functions of the Data + CF-Ack and Data + CF-Poll into a single frame.

The remaining four subtypes of data frames do not in fact carry any user data. The Null Function data frame carries no data, polls, or acknowledgments. It is used only to carry the power management bit in the frame control field to the AP, to indicate that the station is changing to a low-power operating state. The remaining three frames (CF-Ack, CF-Poll, CF-Ack + CF-Poll) have the same functionality as the corresponding data frame subtypes in the preceding list (Data + CF-Ack, Data + CF-Poll,Data + CF-Ack + CF-Poll) but without the data.

Management Frames Management frames are used to manage communications between stations and APs.The following subtypes are included:

- **Association Request:** Sent by a station to an AP to request an association with this BSS. This frame includes capability information, such as whether encryption is to be used and whether this station is pollable.
- **Association Response:** Returned by the AP to the station to indicate whether it is accepting this association request.
- **Reassociation Request:** Sent by a station when it moves from one BSS to another and needs to make an association with the AP in the new BSS. The station uses reassociation rather than simply association so that the new AP knows to negotiate with the old AP for the forwarding of data frames.
- **Reassociation Response:** Returned by the AP to the station to indicate whether it is accepting this reassociation request.
- **Probe Request:** Used by a station to obtain information from another station or AP. This frame is used to locate an IEEE 802.11 BSS.
- **Probe Response:** Response to a probe request.
- **Beacon:** Transmitted periodically to allow mobile stations to locate and identify a BSS.
- **Announcement Traffic Indication Message:** Sent by a mobile station to alert other mobile stations that may have been in low power mode that this station has frames buffered and waiting to be delivered to the station addressed in this frame.
- **Dissociation:** Used by a station to terminate an association.
- **Authentication:** Multiple authentication frames are used in an exchange to authenticate one station to another.
- **Deauthentication:** Sent by a station to another station or AP to indicate that it is terminating secure communications.

11.5 IEEE 802.11 PHYSICAL LAYER

Since its first introduction, the IEEE 802.11 standard has been expanded and revised a number of times. The first version of the standard, simply called IEEE 802.11, includes the MAC layer and three physical layer specifications, two in the 2.4 GHz band (ISM) and one in the infrared, all operating at 1 and 2 Mbps. This version is now obsolete and no longer in use. Table 11.5 summarizes key characteristics of the subsequent revisions. In this section, we survey 802.11b, 802.11a, 802.11g, and 802.11n. The following section deals with 802.11ac and 802.11ad, both of which provide for data rates greater than 1 Gbps.

IEEE 802.11b

One of the original 802.11 standards, now obsolete, used DSSS. It operates in the 2.4 GHz ISM band, at data rates of 1 Mbps and 2 Mbps. In the United States, the FCC requires no licensing for the use of this band. The number of channels available depends on the bandwidth allocated by the various national regulatory agencies.

IEEE 802.11b is an extension of the IEEE 802.11 DSSS scheme, providing data rates of 5.5 and 11 Mbps in the ISM band. The chipping rate is 11 MHz, which is the same as the original DSSS scheme, thus providing the same occupied bandwidth. To achieve a higher data rate in the same bandwidth at the same chipping rate, a modulation scheme known as **complementary code keying (CCK)** is used. The CCK modulation scheme is quite complex and shown in Figure 11.15, but is not examined in detail here.

An optional alternative to CCK is known as packet binary convolutional coding (PBCC). PBCC provides for potentially more efficient transmission at the cost of increased computation at the receiver. PBCC was incorporated into 802.11b in anticipation of its need for higher data rates for future enhancements to the standard.

Physical-Layer Frame Structure IEEE 802.11b defines two physical-layer frame formats, which differ only in the length of the preamble. The long preamble of 144 bits is the same as used in the original 802.11 DSSS scheme and allows

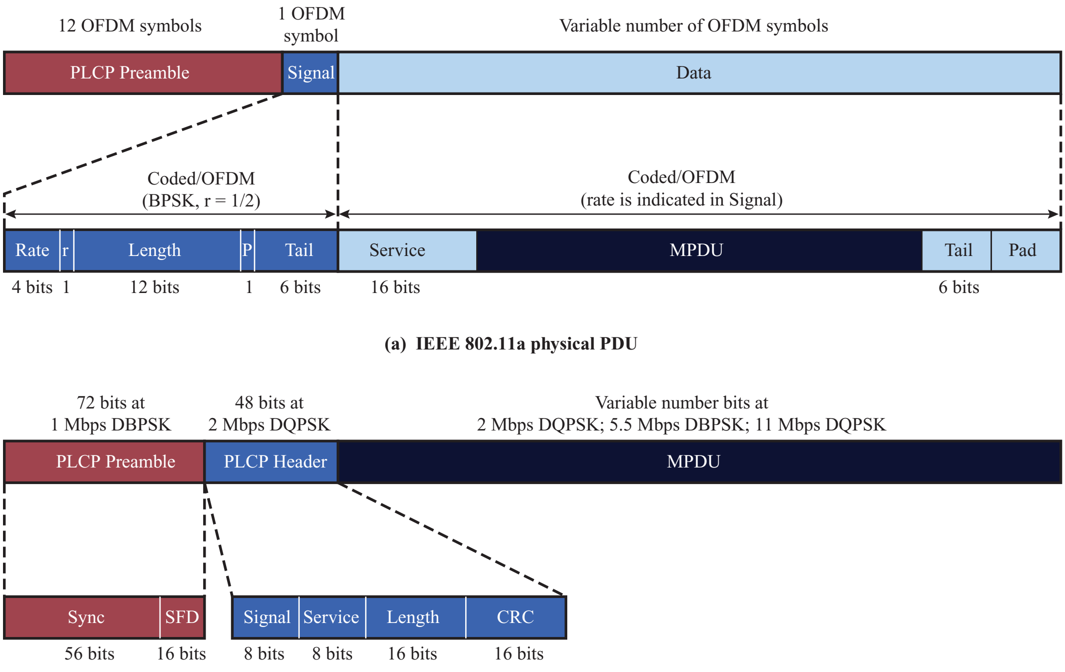
Table 11.5 IEEE 802.11 Physical Layer Standards

Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad
Year introduced	1999	1999	2003	2000	2012	2014
Maximum data transfer speed	54 Mbps	11 Mbps	54 Mbps	65 to 600 Mbps	78 Mbps to 3.2 Gbps	6.76 Gbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz	5 GHz	60 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20, 40 MHz	40, 80, 160 MHz	2160 MHz
Highest order modulation	64 QAM	11 CCK	64 QAM	64 QAM	256 QAM	64 QAM
Spectrum usage	OFDM	DSSS	DSSS, OFDM	OFDM	SC-OFDM	SC, OFDM
Antenna configuration	1 × 1 SISO	1 × 1 SISO	1 × 1 SISO	Up to 4 × 4 MIMO	Up to 8 × 8 MIMO, MU-MIMO	1 × 1 SISO

interoperability with other legacy systems. The short preamble of 72 bits provides improved throughput efficiency. Figure 11.13b illustrates the physical layer frame format with the short preamble. The ***PLCP (physical layer convergence protocol) Preamble*** field enables the receiver to acquire an incoming signal and synchronize the demodulator. It consists of two subfields: a 56-bit ***Sync*** field for synchronization and a 16-bit start-of-frame delimiter (***SFD***). The preamble is transmitted at 1 Mbps using differential BPSK and Barker code spreading.

Following the preamble is the ***PLCP Header***, which is transmitted at 2 Mbps using DQPSK. It consists of the following subfields:

- **Signal:** Specifies the data rate at which the MPDU portion of the frame is transmitted.
- **Service:** Only 3 bits of this 8-bit field are used in 802.11b. One bit indicates whether the transmit frequency and symbol clocks use the same local oscillator. Another bit indicates whether CCK or PBCC encoding is used. A third bit acts as an extension to the Length subfield.
- **Length:** Indicates the length of the MPDU field by specifying the number of microseconds necessary to transmit the MPDU. Given the data rate, the length of the MPDU in octets can be calculated. For any data rate over 8 Mbps, the length extension bit from the Service field is needed to resolve a rounding ambiguity.



(a) IEEE 802.11a physical PDU

(b) IEEE 802.11b physical PDU

Figure 11.13 IEEE 802 Physical-Level Protocol Data Units

- **CRC:** A 16-bit error-detection code used to protect the Signal, Service, and Length fields.

The ***MPDU*** field consists of a variable number of bits transmitted at the data rate specified in the Signal subfield. Prior to transmission, all of the bits of the physical layer PDU are scrambled (see Appendix 11A for a discussion of scrambling).

IEEE 802.11a

Although 802.11b achieved a certain level of success, its limited data rate resulted in limited appeal. To meet the needs for a truly high-speed WLAN, ***IEEE 802.11a*** was developed. Even though it is now obsolete, much of its functionality has been carried over to subsequent 802.11 improvements, so we now investigate some of those details.

Channel Structure IEEE 802.11a makes use of the frequency band called the Universal Networking Information Infrastructure (UNNI), which is divided into three parts. The UNNI-1 band (5.15 to 5.25 GHz) is intended for indoor use; the UNNI-2 band (5.25 to 5.35 GHz) can be used either indoor or outdoor; and the UNNI-3 band (5.725 to 5.825 GHz) is for outdoor use.

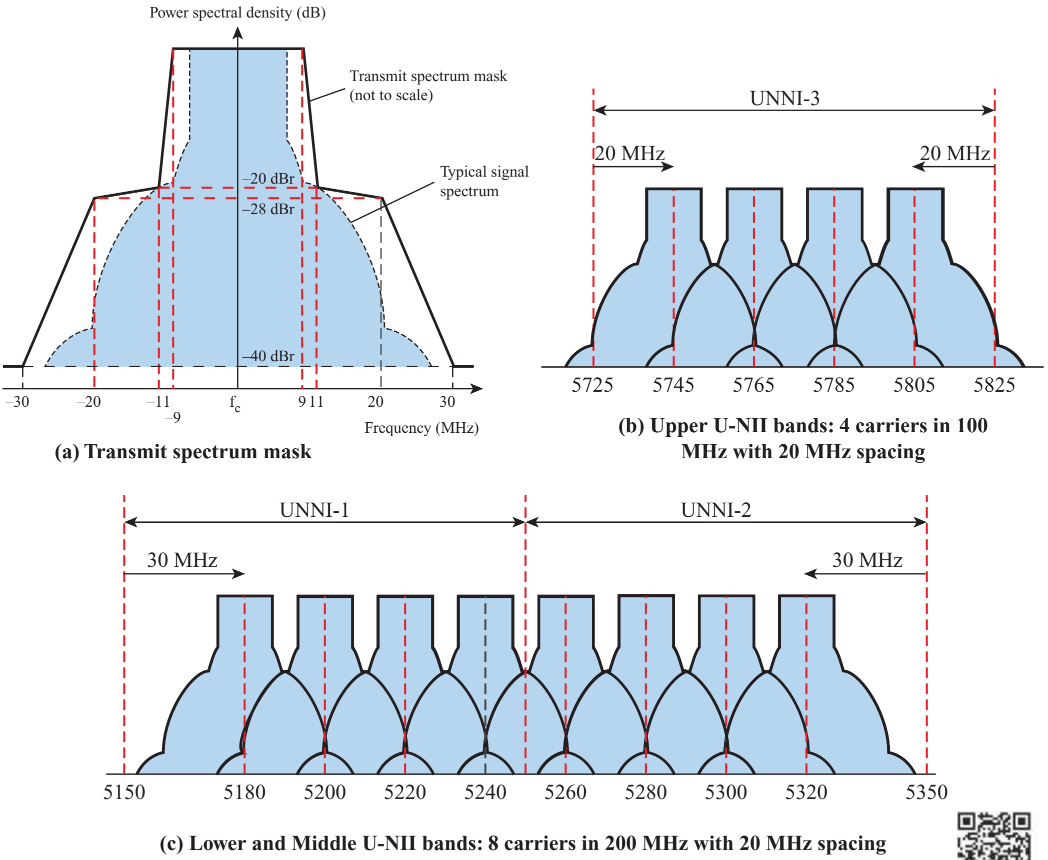
IEEE 802.11a has several advantages over IEEE 802.11b/g:

- IEEE 802.11a utilizes more available bandwidth than 802.11b/g. Each UNNI band provides four nonoverlapping channels for a total of 12 across the allocated spectrum.
- IEEE 802.11a provides much higher data rates than 802.11b and the same maximum data rate as 802.11g.
- IEEE 802.11a uses a different, relatively uncluttered frequency spectrum (5 GHz).

Figure 11.14 shows the channel structure used by 802.11a (and also by 802.11n and 802.11ac which use the 5 GHz bands). The first part of the figure indicates a transmit spectrum mask, which is defined in 802.11b as follows: The transmitted spectrum mask shall have a 0 dBr (dB relative to the maximum spectral density of the signal) bandwidth not exceeding 18 MHz (9 MHz offset), −20 dBr at 11 MHz frequency offset, −28 dBr at 20 MHz frequency offset, and −40 dBr at 30 MHz frequency offset and above. The transmitted spectral density of the transmitted signal shall fall within the spectral mask. A typical signal spectrum is shown. The purpose of the spectrum mask is to constrain the spectral properties of the transmitted signal such that signals in adjacent channels do not interfere with one another.

Coding and Modulation Unlike the 2.4 GHz specifications, IEEE 802.11a does not use a spread spectrum scheme but rather uses OFDM. OFDM, also called multicarrier modulation, uses multiple carrier signals at different frequencies, sending some of the bits on each channel. It is discussed in Chapter 8. This is similar to FDM. However, in the case of OFDM, all of the subchannels are dedicated to a single data source.

To complement OFDM, the specification supports the use of a variety of modulation and coding alternatives. The system uses up to 48 subcarriers that are



(a) Transmit spectrum mask

(b) Upper U-NII bands: 4 carriers in 100 MHz with 20 MHz spacing

(c) Lower and Middle U-NII bands: 8 carriers in 200 MHz with 20 MHz spacing

Figure 11.14 IEEE 802.11a Channel Scheme

modulated using BPSK, QPSK, 16-QAM, or 64-QAM. Subcarrier frequency spacing is 0.3125 MHz and each subcarrier transmits at a rate of 250 kbaud. A convolutional code at a rate of 1/2, 2/3, or 3/4 provides forward error correction (FEC). The combination of modulation technique and coding rate determines the data rate.

Physical-Layer Frame Structure The primary purpose of the physical layer is to transmit MPDUs as directed by the 802.11 MAC layer. The PLCP sublayer provides the framing and signaling bits needed for the OFDM transmission and the PMD sublayer performs the actual encoding and transmission operation.

Figure 11.13a illustrates the physical layer frame format. The ***PLCP Preamble*** field enables the receiver to acquire an incoming OFDM signal and synchronize the demodulator. Next is the ***Signal*** field, which consists of 24 bits encoded as a single OFDM symbol. The Preamble and Signal fields are transmitted at 6 Mbps using BPSK. The signal field consists of the following subfields:

- **Rate:** Specifies the data rate at which the data field portion of the frame is transmitted.
- **r:** reserved for future use.

- **Length:** Number of octets in the MAC PDU.
- **P:** An even parity bit for the 17 bits in the Rate, r, and Length subfields.
- **Tail:** Consists of 6 zero bits appended to the symbol to bring the convolutional encoder to zero state.

The ***Data*** field consists of a variable number of OFDM symbols transmitted at the data rate specified in the Rate subfield. Prior to transmission, all of the bits of the Data field are scrambled (see Appendix 11A for a discussion of scrambling). The Data field consists of four subfields:

- **Service:** Consists of 16 bits, with the first 7 bits set to zeros to synchronize the descrambler in the receiver, and the remaining 9 bits (all zeros) reserved for future use.
- **MAC PDU:** Handed down from the MAC layer. The format is shown in Figure 11.12.
- **Tail:** Produced by replacing the six scrambled bits following the MPDU end with 6 bits of all zeros; used to reinitialize the convolutional encoder.
- **Pad:** The number of bits required to make the Data field a multiple of the number of bits in an OFDM symbol (48, 96, 192, or 288).

IEEE 802.11g

IEEE 802.11g extends 802.11b to data rates above 20 Mbps, up to 54 Mbps. Like 802.11b, 802.11g operates in the 2.4 GHz range and thus the two are compatible. The standard is designed so that 802.11b devices will work when connected to an 802.11g AP, and 802.11g devices will work when connected to an 802.11b AP, in both cases using the lower 802.11b data rate.

IEEE 802.11g offers a wide array of data rate and modulation scheme options. IEEE 802.11g provides compatibility with 802.11 and 802.11b by specifying the same modulation and framing schemes as these standards for 1, 2, 5.5, and 11 Mbps. At data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, 802.11g adopts the 802.11a OFDM scheme, adapted for the 2.4 GHz rate; this is referred to as ERP-OFDM, with ERP standing for extended rate physical layer. In addition, an ERP-PBCC scheme is used to provide data rates of 22 and 33 Mbps.

The IEEE 802.11 standards do not include a specification of speed versus distance objectives. Different vendors will give different values, depending on the environment. Table 11.6, based on [LAYL04], gives estimated values for a typical office environment.

IEEE 802.11n

With increasing demands being placed on WLANs, the 802.11 committee looked for ways to increase the data throughput and overall capacity of 802.11 networks. The goal of this effort was to not just increase the bit rate of the transmitting antennas but to increase the effective throughput of the network. Increasing effective throughput involves not only looking at the signal encoding scheme, but also at the antenna architecture and the MAC frame structure. The result of these efforts is

Table 11.6 Estimated Distance (m) Versus Data Rate

Data Rate (Mbps)	802.11b	802.11a	802.11g
1	90+	—	90+
2	75	—	75
5.5(b)/6(a/g)	60	60+	65
9	—	50	55
11(b)/12(a/g)	50	45	50
18	—	40	50
24	—	30	45
36	—	25	35
48	—	15	25
54	—	10	20

a package of improvements and enhancements embodied in IEEE 802.11n. This standard is defined to operate in both the 2.4 GHz and the 5 GHz bands and can therefore be made upwardly compatible with either 802.11a or 802.11b/g.

IEEE 802.11n embodies changes in three general areas: use of MIMO, enhancements in radio transmission, and MAC enhancements. We examine each of these in the following subsections.

Multiple-Input-Multiple-Output MIMO antenna architecture is a major enhancement provided by 802.11n. Discussions of MIMO are provided in Chapters 5 and 6, so we content ourselves with a brief overview. In a MIMO scheme, the transmitter employs multiple antennas. MIMO can provide multiple types of benefits, by using multiple parallel streams, beamforming, diversity, or multiuser MIMO. The first three capabilities are supported in 802.11n (some optionally), and the use of at least two parallel streams is required from the AP [PERA08].

The source data stream is divided into *n* substreams, one for each of the *n* transmitting antennas. The individual substreams are the input to the transmitting antennas (multiple input). At the receiving end, *m* antennas receive the transmissions from the *n* source antennas via a combination of line-of-sight transmission and multipath. The outputs from the *m* receiving antennas (multiple output) are combined. With a lot of complex math, the result is a much better received signal than can be achieved with either a single antenna or multiple frequency channels. 802.11n defines a number of different combinations for the number of transmitters and the number of receivers, from 2×1 to 4×4. Each additional transmitter or receiver in the system increases the SNR (signal-to-noise ratio). A simplified computation would say that four parallel streams would increase the total transmitted data rate approximately by a factor of 4.

Due to the inherent cost of multiple antennas, three or four spatial streams from the AP are not required, and only one spatial stream is required from the station. The standard also supports optional features such as four streams in both directions, transmit beamforming, and space-time block coding to improve diversity reliability.

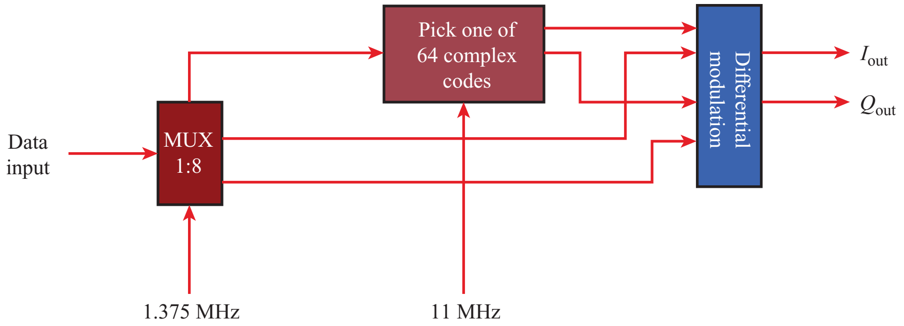


Figure 11.15 11-Mbps CCK Modulation Scheme

Radio Transmission Schemes In addition to MIMO, 802.11n makes a number of changes to the radio transmission scheme to increase capacity. The most significant of these techniques, known as channel bonding, combines two 20 MHz channels to create a 40 MHz channel. Using OFDM, this allows for a little more than twice as many subchannels, more than doubling the transmission rate. When a 40 MHz channel is created, it is formed from two adjacent 20 MHz channels. Each 20 MHz channel reserves some bandwidth at the edges to avoid interference, but when these are combined, the extra bandwidth in between the channels can be used. The effect is that 802.11n achieves slightly more than double the rate with 40 MHz channels. 802.11a and 802.11g used 48 subcarriers per 20 MHz, but 802.11n defined 108 per 40 MHz, 2.25 times the original bandwidth.

802.11a and 802.11g use OFDM symbols that last 4 μs. For the highest rate of 54 Mbps, 216 bits per symbol are spread out over 48 subcarriers. Also included is an 800 ns guard interval (used for the OFDM cyclic prefix), hopefully confining multipath effects to that time interval. This 54 Mbps rate uses 64 QAM and 72 additional error-correction bits; 216 data bits are used out of the total 216 + 72 bits resulting in a $\frac{3}{4}$ coding rate. 802.11n continues to use this 4 μs symbol, but also allows for better channel conditions. In cases where multipath is not as significant, a 400 ns guard interval can be used, reducing the symbol time to 3.6 μs. This improves the data rate by 11%. 802.11n increases the highest encoding rate to 5/6, for another 11% increase. The final result is a maximum of 150 Mbps per 40 MHz, and 600 Mbps for 4 parallel streams.

In addition to these maximum data rates, 802.11n provides 32 different modulation and coding (MCS) combinations where the AP and the station work together to estimate channel conditions and find the best fit. There are several other MCS combinations that are also supported if the AP and station use different schemes when they transmit, because the channel quality from the AP to the station might be different than in the reverse direction.

In some cases, 802.11n devices will have to operate alongside legacy devices, in which case there will be some reductions in efficiency. First of all, 802.11n devices must sense legacy devices and might only be able to use 20 MHz if others are active. Also, the legacy devices need to recognize 802.11n, so 802.11n headers need to include extra headers that are encoded at lower data rates that legacy devices can read to recognize that 802.11n devices are using the channels and for how long. Additionally, 802.11n must send RTS/CTS or CTS-to-self messages. 802.11n also supports, however, a high throughput mode (also known as *greenfield* operation), where these headers and RTS/CTS messages do not need to be included if an environment is free of legacy devices.

MAC Enhancements As the data rate of a physical layer increases, the effective throughput of a protocol is still limited by its overhead. 802.11 overhead involves protocol header bits, backoffs, and IFS times.

802.11n provides some MAC enhancements. The most significant change is to aggregate multiple MAC frames into a single block for transmission. Once a station acquires the medium for transmission, it is allowed to transmit long packets without significant delays between transmissions. Throughput is affected if every frame requires an ACK, along with the DIFS and SIFS times between every frame. Instead, with 802.11n the receiver can send a single block acknowledgment. The physical header associated with transmission is sent only at the beginning of the aggregated frame, rather than one physical header per individual frame. Frame aggregation can result in significantly improved efficient use of the transmission capacity. Each frame no longer requires its own ACK and the associated IFS times.

The 802.11n specification includes three forms of aggregation, illustrated in Figure 11.16 [CISC14]. For simplicity, the 4-octet MAC trailer field is not shown. Aggregation either combines MSDUs, MPDUs, or both. Recall that MSDUs come down from the LLC layer and MPDUs from the MAC layer. A-MSDU aggregation combines multiple MSDUs into a single MPDU. Thus there is a single MAC header and single FCS for all of the MSDUs rather than for each of the MSDUs. This provides a certain amount of efficiency because the 802.11 MAC header is potentially quite lengthy. However, if a bit error occurs in one of the MSDUs, all of the aggregated MSDUs must be retransmitted, as seen in Figure 11.16b. A-MPDU aggregation combines multiple MPDUs in a single physical transmission. Thus, as with A-MSDU, only a single physical-layer header is needed. This approach is less efficient because each MPDU includes the MAC header and FCS. However, if a bit error occurs in one of the MPDUs, only that MPDU needs to be retransmitted. Finally, the two forms of aggregation can be combined (A-MPDU of A-MSDU).

If aggregation is not used, 802.11n can use a new 2 μs reduced interframe space (RIFS) between packets when transmitted in a group, instead of an SIFS of 10 μs for 2.4 GHz or 16 μs for 2.4 GHz. This feature, however, did not prove as useful as aggregation and was not carried forward into the later 802.11 enhancements discussed next.

11.6 GIGABIT WI-FI

Just as there has been a need to extend the Ethernet wired LAN standard to speeds in the gigabit per second range, the same requirement exists for Wi-Fi. Accordingly, IEEE 802.11 has recently introduced two new standards, 802.11ac and 802.11ad, which provide for Wi-Fi networks that operate at well in excess of 1 Gbps. We look at these two standards in turn.

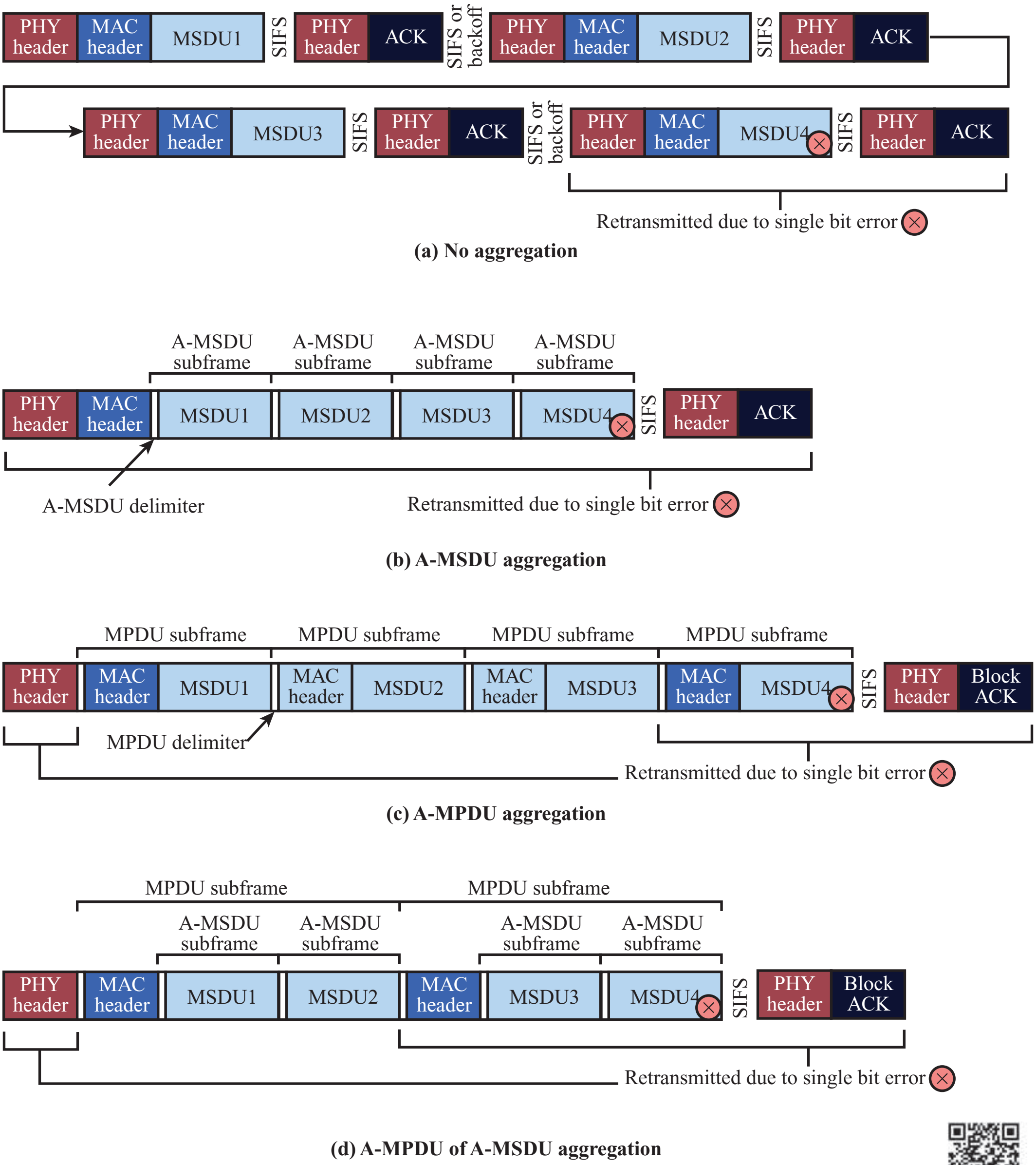


Figure 11.16 Forms of Aggregation

IEEE 802.11ac

IEEE 802.11ac operates in the channels in the 5 GHz band as illustrated in Figure 11.14, as does 802.11a and 802.11n. It is designed to provide a smooth evolution from 802.11n. The new standard achieves much higher data rates than 802.11n by means of enhancements in three areas (as seen in the three axes of Figure 11.17):

- **Bandwidth:** The maximum bandwidth of 802.11n is 40 MHz; the maximum bandwidth of 802.11ac is 160 MHz.

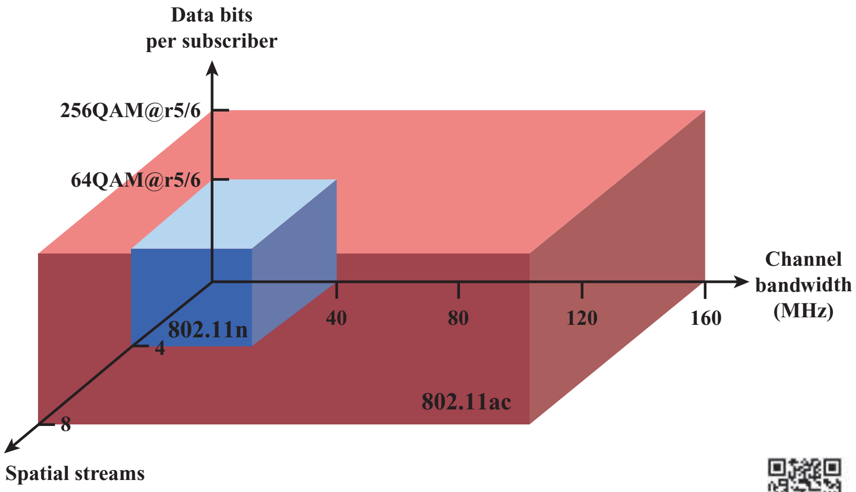


Figure 11.17 IEEE 802.11 Performance Factors

- **Signal encoding:** 802.11n can use 64 QAM with OFDM, and 802.11ac can use 256 QAM with OFDM. Thus, more bits can be encoded per symbol. Both schemes use forward error correction with a code rate of 5/6 (ratio of data bits to total bits).
- **MIMO:** With 802.11n, there can be a maximum of 4 channel input and 4 channel output antennas. 802.11ac increases this to 8 × 8.

We can quantify these enhancements using the following formula, which yields the physical layer data rate in bps:

$$\text{Data rate} = \frac{(\text{number of data subcarriers}) \times (\text{number of spatial streams}) \times (\text{data bits per subcarrier})}{(\text{time per OFDM symbol, in seconds})}$$

Using this equation, we have the following maximum data rates:

$$\text{802.11n: } \frac{108 \times 4 \times (5/6 \times \log_2 64)}{3.6 \times 10^{-6}} = 600 \times 10^6 \text{ bps} = 600 \text{ Mbps}$$

$$\text{802.11ac: } \frac{468 \times 8 \times (5/6 \times \log_2 256)}{3.6 \times 10^{-6}} = 6937 \times 10^6 \text{ bps} = 6.937 \text{ Gbps}$$

Increasing the channel bandwidth by a factor of 4 increases the data rate by a factor of 4.33, because the number of subcarriers expands from 108 to 468. The transmit power must now be spread over four times as many subcarriers, however, resulting in a slight reduction in range. Going from 64 QAM to 256 QAM increases the data rate by a factor of 1.33. However, 256 QAM is more sensitive to noise and thus is only effective at shorter ranges. Finally, the speed is directly proportional to the number of spatial streams. Of course, more spatial streams require more antennas, increasing the cost of the subscriber device.

Bandwidth Expansion Support for 80 MHz and 160 MHz channels requires extensions to CSMA techniques, spectrum considerations, and new RTS-CTS procedures.

- **CSMA Techniques:** 802.11ac devices set primary channels and perform standard clear channel assessment procedures over those channels. Then they use other procedures to see if additional secondary channels can be used to expand the bandwidth to up to 160 MHz. These procedures for secondary channels are less complex and use less overhead, but are more sensitive to signal energy that might be present. If the full bandwidth is not available, the device may restart the contention and backoff process. However, 802.11ac devices may also dynamically adjust their bandwidth allocations in every frame according to channels that are available.
- **Spectrum Considerations:** The 5 GHz ISM bands are less congested, which helps limit interference for 802.11ac. Figure 11.18 shows the channelization of possible frequency bands. Note that there are only two possible contiguous sets of frequencies for a 160 MHz channel. Therefore, 802.11ac supports an 80 + 80 MHz format where two noncontiguous 80 MHz bands can be combined.
- **RTS-CTS:** In order to test if, for example, the 80 MHz of a requested channel is available, the initiator senses for activity on each of those four 20 MHz channels and sends an RTS on each (so also 8 RTSs for 160 MHz). The 802.11ac RTS format that is used includes the requested bandwidth. The receiver of the RTS then also senses if anyone is actively using any of those channels. Figure 11.19 illustrates two possible scenarios that could result. The receiver will respond with CTSs to indicate available bandwidth (20, 40, or 80 MHz, but not 60 MHz); these CTSs will also be sent in 802.11a format on each free

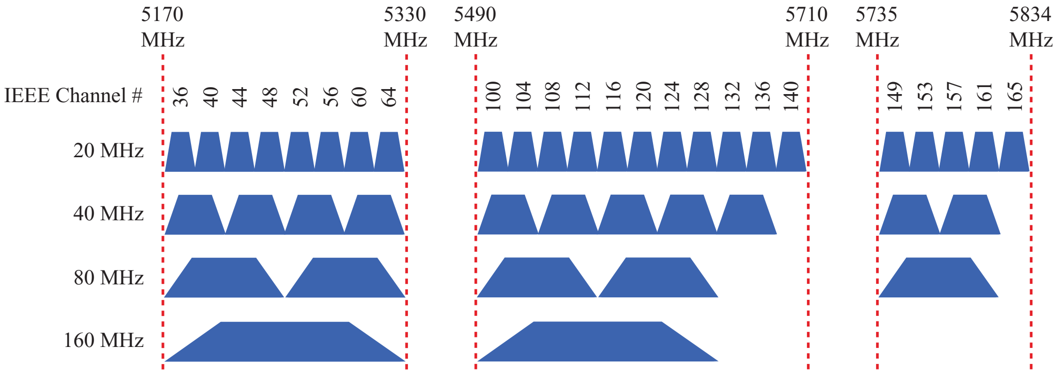


Figure 11.18 5 GHz 802.11ac Channel Allocations

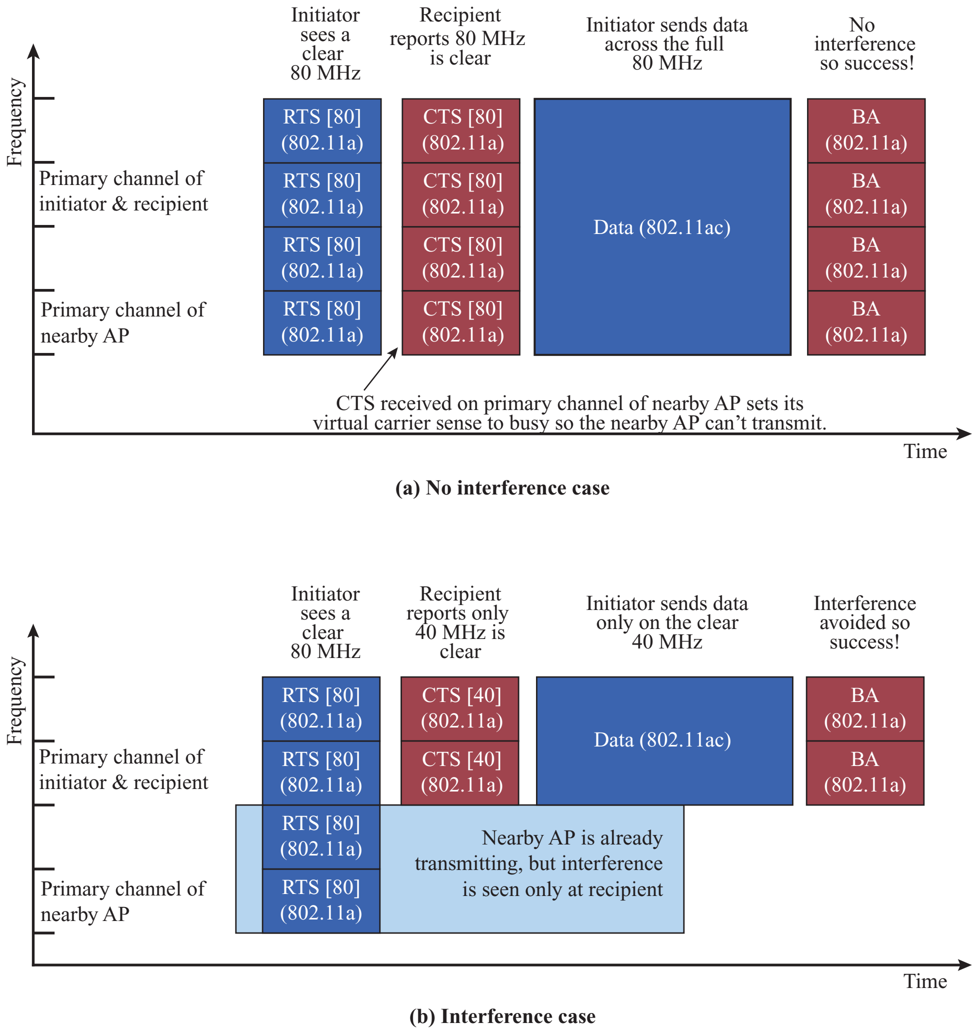

Initiator sees a clear 80 MHz
Recipient reports 80 MHz is clear
Initiator sends data across the full 80 MHz
No interference so success!
Frequency
Primary channel of initiator & recipient
Primary channel of nearby AP
RTS [80] (802.11a)
CTS [80] (802.11a)
Data (802.11ac)
BA (802.11a)
CTS received on primary channel of nearby AP sets its virtual carrier sense to busy so the nearby AP can't transmit.
Time
(a) No interference case
Initiator sees a clear 80 MHz
Recipient reports only 40 MHz is clear
Initiator sends data only on the clear 40 MHz
Interference avoided so success!
CTS [40] (802.11a)
Nearby AP is already transmitting, but interference is seen only at recipient
(b) Interference case

Figure 11.19 RTS/CTS Enhanced with Bandwidth Signaling

20 MHz channel to respond to the RTS. All 802.11a/n/ac devices will see and decode this CTS message so they can wait.

Multiuser MIMO In addition to expansion of 802.11n techniques to 8 × 8 MIMO, 802.11ac includes the option of multiuser MIMO (MU-MIMO). This means that on the downlink, the transmitter is able to use its antenna resources to transmit multiple frames to different stations, all at the same time and over the same frequency spectrum. Thus, an MU-MIMO AP can simultaneously communicate with multiple single-antenna devices on the same frequency. Single antennas are common on smartphones and tablets. This enables the AP to deliver significantly more data in many environments while keeping the complexity on the device side minimal.

Directional antennas not only can direct the signal but can also point antenna pattern nulls in other directions. For example, if MU-MIMO is directed toward three stations, the first beam might point strongly toward user 1 and with very little gain toward users 2 and 3. And the other two beams would be directed accordingly. The AP must know the quality of the wireless channel very accurately for this to work effectively, even as the channel is changing with time. This is especially challenging for moving mobile devices.

802.11n had a variety of possible mechanisms, but 802.11ac has a more consistent approach to ensure interoperability. Typically an AP sends a "Very High Throughput Null Data Packet Announcement" (VHT NDPA) that simply sends the address of the AP to intended recipients. After an SIFS, a "VHT Null Data Packet" (VHT NDP) is sent to perform *sounding*, which involves the AP sending training symbols that receivers use to measure channel conditions. The intended recipients use the preamble (a known sequence of bits at the beginning of the frame) of the VHT NDP to measure the RF channel. Then they respond with "VHT Compressed Beamforming" messages that are used to adjust the MIMO steering matrix (see Chapter 6). Ideally many measurements would be taken with a lot of detail in the measurements, but this creates high overhead. So the measurement information is compressed and an AP must send an appropriate number of messages.

Other PHY and MAC Enhancements FEC is implemented in 802.11ac using required PBCC or optional low density parity check (LDPC) codes. Space-time Block Coding can also be used along with MIMO as in 802.11n, but with fewer of those modes possible. Another difference for 802.11ac is that every transmission is required to be sent as an A-MPDU aggregate. This was introduced in 802.11n (see above) and was made mandatory in 802.11ac along with a larger maximum frame size. Other than the RTS/CTS modifications, this is the only significant modification to the MAC layer from 802.11n.

The Wi-Fi Alliance has taken a two-phase process in certification of 802.11ac products, related to which features are required and optional. "Wave 1" products provide rates up to 1.3 Gbps using 256 QAM, 80 MHz channels, and 3 spatial streams. "Wave 2" products are likely to additionally provide 160 MHz channels, 4 spatial streams, and MU-MIMO [CISC14].

IEEE 802.11ad

IEEE 802.11ad, using the name ***WiGig***, is a version of 802.11 operating in the 60 GHz frequency band. This band offers the potential for much wider channel bandwidth than the 5 GHz band, enabling high data rates up to 7 Gbps with relatively simple signal encoding and antenna characteristics. This enables a series of high bandwidth applications; WiGig also supplies ***Protocol Adaptation Layers*** (***PALs***). There are audio/visual PALs to support HDMI and DisplayPort, and there are input/output PALs for SD, USB, and PCIe.

Few devices operate in the 60 GHz band, which means communications would experience less interference than in the other bands used by 802.11. However, at

60 GHz, 802.11ad is operating in the millimeter range, which has some undesirable propagation characteristics:

1. Free space loss increases with the square of the frequency [Equation (5.1)]; thus losses are much higher in this range (20 dB more from 6 GHz and 60 GHz) than in the ranges used for traditional microwave systems.
2. Multipath losses can be quite high. Reflection occurs when an electromagnetic signal encounters a surface that is large relative to the wavelength of the signal; scattering occurs if the size of an obstacle is on the order of the wavelength of the signal or less; diffraction occurs when the wavefront encounters the edge of an obstacle that is large compared to the wavelength.
3. Millimeter-wave signals generally don't penetrate solid objects.

For these reasons, 802.11ad is likely to be useful only within a single room. Because it can support high data rates and, for example, could easily transmit uncompressed high-definition video, it is suitable for applications such as replacing wires in a home entertainment system, or streaming high-definition movies from your cell phone to your television. It could also be used in an office environment for streaming video to a projector or between laptops and tablets in a conference room.

Adaptive beamforming of high gain directional antennas is used in 802.11ad to overcome the propagation loss. As seen in Chapter 6, directional beams can greatly increase antenna gain using MIMO. The 802.11ad beamforming process is supported through the MAC and PHY layers to establish basic course level communication through the sector level sweep (SLS) and then to fine-tune the settings through the beam refinement process (BRP). Because 60 GHz transmission is highly dependent on line-of-sight, a person walking in between the two stations can disrupt the communication. But the 802.11ad devices can quickly adapt their beams to an alternate path, even finding paths off reflections from walls or other objects.

The striking difference between 802.11ac and 802.11ad is the channel bandwidth. Instead of a 160 MHz maximum, 802.11ad has a huge channel bandwidth of 2160 MHz, centered at 58.32, 60.48, 62.64, and 64.8 GHz (not all channels are available depending on the country).

802.11ad PHY Layer IEEE 802.11ad defines four physical layer modulation and coding schemes (Table 11.7). Each type has a distinct purpose and supports a different range of data rates.

Control PHY (CPHY) is by far the most robustly coded (and consequently, lowest throughput) mode, with a code rate of only 1/2. Its purpose is exclusively to transmit control channel messages. The CPHY robustness is evident from its use of differential encoding, code spreading, and BPSK modulation. Differential encoding eliminates the need for carrier tracking, 32× spreading contributes a theoretical 15 dB gain to the link budget, and BPSK is very noise tolerant.

As with CPHY, ***single carrier PHY (SCPHY)*** uses the powerful LDPC code for robust forward error correction and provides three options for modulation. The set of options for code rate and modulation density allow for a trade-off between throughput and robustness to be determined operationally. Rates up to 4.62 Gbps can be achieved.

OFDM PHY (OFDMPHY) employs multicarrier modulation, which can provide higher modulation densities and hence higher data throughput than the

Table 11.7 IEEE 802.11ad Modulation and Coding Schemes

Physical Layer	Coding	Modulation	Raw Bit Rate
Control (CPHY)	1/2 LDPC, 32 × spreading	$\pi/2$-DBPSK	27.5 Mbps
Single carrier (SCPHY)	1/2 LDPC 1/2 LDPC, 5/8 LDPC 3/4 LDPC 13/16 LDPC	$\pi/2$-BPSK, $\pi/2$-QPSK, π 2-16 QAM	385 Mbps to 4.62 Gbps
OFDM (OFDMPHY)	1/2 LDPC, 5/8 LDPC 3/4 LDPC 13/16 LDPC	OFDM-OQPSK OFDM-QPSK OFDM-16 QAM OFDM-64 QAM	693 Mbps to 6.76 Gbps
Low-power single carrier (LPSCPHY)	RS(224,208) + Block Code(16/12/9/8,8)	$\pi/2$-BPSK, $\pi/2$-QPSK	636 Mbps to 2.5 Gbps

BPSK = binary phase-shift keying
DBPSK = differential binary phase-shift keying
LDPC = low density parity check code
OFDM = orthogonal frequency-division multiplexing
OQPSK = offset quadrature phase-shift keying
QAM = quadrature amplitude modulation
QPSK = quadrature phase-shift keying
RS = Reed-Solomon

single-carrier options, up to 6.756 Gbps. As with SCPHY, OFDMPHY provides a choice of error protection ratio and the depth of modulation applied to the OFDM data carriers, again to provide operational control over the robustness/throughput trade-off. The choice between SCPHY and OFDMPHY depends on several factors. OFDM modulation will generally impose greater power requirements than SCPHY, but is more robust in the presence of multipath distortion.

The LDPC error-correcting coding technique that is common to the CPHY, SCPHY, and OFDMPHY is based on a common codeword length of 672 bits carrying 336, 504, 420, or 546 payload bits to achieve a code rate of 1/2, 3/4, 5/8, or 13/16 as required.

Low-power single carrier (LPSCPHY) employs single-carrier modulation to minimize power consumption. It also uses either Reed-Solomon or Hamming block codes, which require less IC area and hence less power than LDPC, at the expense of less robust error correction. Small battery-powered devices could benefit from the extra power savings.

802.11ad MAC Layer The 802.11ad/WiGig MAC layer provides a series of necessary new and enhanced features.

- Network architecture: Instead of going through an AP, a new network architecture called the ***Personal BSS*** (***PBSS***) is provided that easily enables devices to talk directly with each other. Peer-to-peer 802.11 communication is also possible through an IBSS, but in the PBSS one node assumes the role of a PBSS control point to provide basic timing and allocation of service periods and contention-based access periods. This PBSS usage model would be common in WiGig, for example, between multimedia distribution and display devices.

- Seamless multiband operation: Allow seamless switching to and from 60 and 2.4/5 GHz operation to adapt to availability of 60 GHz channels.
- Power management: 802.11ad provides a new scheduled access mode to reduce power consumption. Devices can schedule between themselves when they are to communicate, then sleep otherwise.
- Advanced security: WiGig devices will use Galois/Counter mode, which supports higher speed communication through highly efficient calculations.

11.7 OTHER IEEE 802.11 STANDARDS

In addition to the standards so far discussed, which provide specific physical layer functionality, a number of other 802.11 standards have been issued or are in the works. Refer to Table 11.1 for the complete list.

IEEE 802.11e makes revisions to the MAC layer to improve quality of service and address some security issues. It accommodates time-scheduled and polled communication during null periods when no other data are being sent. In addition, it offers improvements to the efficiency of polling and enhancements to channel robustness. These enhancements should provide the quality required for such services as IP telephony and video streaming. Any station implementing 802.11e is referred to as a QoS station, or QSTA. In a QSTA, the DCF and PCF (Figure 11.9) modules are replaced with a hybrid coordination function (HCF). The HCF consists of enhanced distributed channel access (EDCA) and HCF controlled channel access (HCCA). EDCA is an extension of the legacy DCF mechanism to include priorities. As with the PCF, HCCA centrally manages medium access, but does so in a more efficient and flexible manner.

IEEE 802.11i defines security and authentication mechanisms at the MAC layer. This standard is designed to address security deficiencies in the wire equivalent privacy (WEP) mechanism originally designed for the MAC layer of 802.11. The 802.11i scheme uses stronger encryption and other enhancements to improve security and is discussed in Section 11.8.

IEEE 802.11k defines Radio Resource Measurement enhancements that provide mechanisms available to higher protocol layers for radio and network measurements. The standard defines what information should be made available to facilitate the management and maintenance of wireless and mobile LANs. Among the data provided are the following:

- To improve roaming decisions, an AP can provide a site report to a station when it determines that the station is moving away from it. The site report is an ordered list of APs, from best to worst service that a station can use in changing over to another AP.
- An AP can collect channel information from each station on the WLAN. Each station provides a noise histogram that displays all non-802.11 energy on that channel as perceived by the station. The AP also collects statistics on how long a channel is used during a given time. These data enable the AP to regulate access to a given channel.

- APs can query stations to collect statistics, such as retries, packets transmitted, and packets received. This gives the AP a more complete view of network performance.
- 802.11k extends the transmit power control procedures defined in 802.11h to other regulatory domains and frequency bands, to reduce interference and power consumption and to provide range control.

IEEE 802.11m is an ongoing task group activity to correct editorial and technical issues in the standard. The task group reviews documents generated by the other task groups to locate and correct inconsistencies and errors in the 802.11 standard and its approved amendments.

802.11p provides wireless access for the vehicular environment. It allows for communication between devices moving up to 200 km/hr (124.3 mi/hr). Devices do not need to associate or authenticate with each other. Instead, they just join the overall WAVE (Wireless Access in Vehicular Environments) network in the area. Lower data rates are used, because movement can cause more packet errors. 802.11p also allows for greater output power to accommodate longer distances.

IEEE 802.11r provides a fast roaming capability. Devices may register in advance with a neighbor AP, so security and quality of service settings can be negotiated before the device needs to switch to a new AP. The duration of connectivity loss can be substantially reduced.

IEEE 802.11s defines MAC procedures for 802.11 devices to use multi-hop communication to support a wireless LAN mesh topology. Devices mutually serve as wireless routers. The amendment supports unicast, multicast, and broadcast packet delivery.

IEEE 802.11z provides Tunneled Direct Link Setup, which allows devices to avoid the delays and contention process for going through an AP. Higher order modulation schemes could also be used if the devices are closer to each other than with an AP. 802.11z is an extension of features in 802.11e and defines a special Ethertype frame to tunnel setup messages through a legacy AP. Frequency offloading can also be used to switch to empty frequencies.

IEEE 802.11aa provides improved multimedia performance to enhance 802.11e capabilities. The enhancements include groupcast with retries for new transmission policies for group addressed frames and intra-access category prioritization to further clarify and create subcategories. It also includes a stream classification service to arbitrarily map streams to queues and solutions to overlapping BSS management problems by performing channel selection and cooperative resource sharing.

11.8 IEEE 802.11I WIRELESS LAN SECURITY

Wireless networks, and the wireless devices that use them, introduce a host of security problems over and above those found in wired networks. Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include the following [MA10]:

- **Channel:** Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks. Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols.

- **Mobility:** Wireless devices are, in principal and usually in practice, far more portable and mobile than wired devices. This mobility results in a number of risks, described subsequently.
- **Resources:** Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware.
- **Accessibility:** Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks.

In simple terms, the wireless environment consists of three components that provide point of attack.

- **Client:** The wireless client can be a cell phone, a Wi-Fi-enabled laptop or tablet, a wireless sensor, a Bluetooth device, and so on.
- **Access Point:** The wireless access point provides a connection to the network or service. Examples of access points are cell towers, Wi-Fi hotspots, and wireless access points to wired local or wide area networks.
- **Wireless Medium:** The transmission medium, which carries the radio waves for data transfer, is also a source of vulnerability.

There are two characteristics of a wired LAN that are not inherent in a wireless LAN.

1. In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a wireless LAN, any station within the radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN in that it requires some positive and presumably observable action to connect a station to a wired LAN.
2. Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN. On the other hand, with a wireless LAN, any station within the radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

These differences between wired and wireless LANs suggest the increased need for robust security services and mechanisms for wireless LANs. The original 802.11 specification included a set of security features for privacy and authentication that were quite weak. For privacy, 802.11 defined the **Wired Equivalent Privacy (WEP)** algorithm. The privacy portion of the 802.11 standard contained major weaknesses. Subsequent to the development of WEP, the 802.11i task group has developed a set of capabilities to address the WLAN security issues. In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated **Wi-Fi Protected Access (WPA)** as a Wi-Fi standard. WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard. The final form of the 802.11i standard is referred to as ***Robust Security Network (RSN)***. The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.

The RSN specification is quite complex, and occupies 145 pages of the 2012 IEEE 802.11 standard. In this section, we provide an overview.

IEEE 802.11i Services

The 802.11i RSN security specification defines the following services:

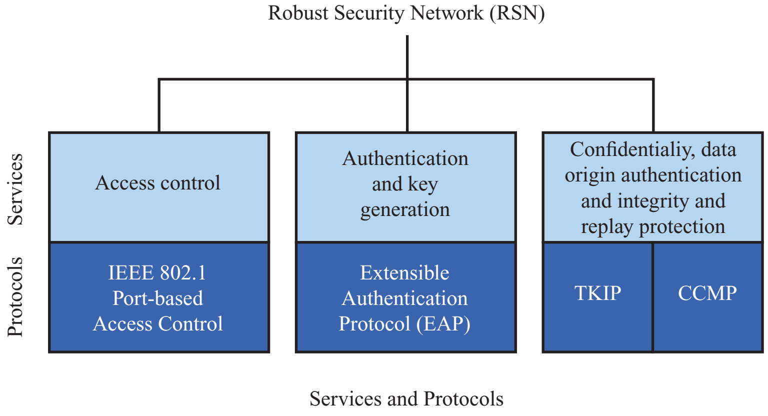
- **Authentication:** A protocol is used to define an exchange between a user and an **authentication server (AS)** that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
- **Access control**[4]**:** This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.
- **Privacy with message integrity:** MAC-level data (e.g., an LLC PDU) are encrypted along with a message integrity code that ensures that the data have not been altered.

Figure 11.20 indicates the security protocols used to support these services.

IEEE 802.11i Phases of Operation

The operation of an IEEE 802.11i RSN can be broken down into five distinct phases of operation as seen in Figure 11.21. The exact nature of the phases will depend on the configuration and the end points of the communication. Possibilities include (referencing the ESS architecture in Figure 11.8) the following:

1. Two wireless stations in the same BSS communicating via the access point (AP) for that BSS.


Robust Security Network (RSN)
Services
Protocols
Access control
Authentication and key generation
Confidentialiy, data origin authentication and integrity and replay protection
IEEE 802.1 Port-based Access Control
Extensible Authentication Protocol (EAP)
TKIP
CCMP
Services and Protocols

CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Figure 11.20 Elements of IEEE 802.11i

[4] In this context, we are discussing access control as a security function. This is a different function than MAC as described in Section 11.4. Unfortunately, the literature and the standards use the term access control in both contexts.

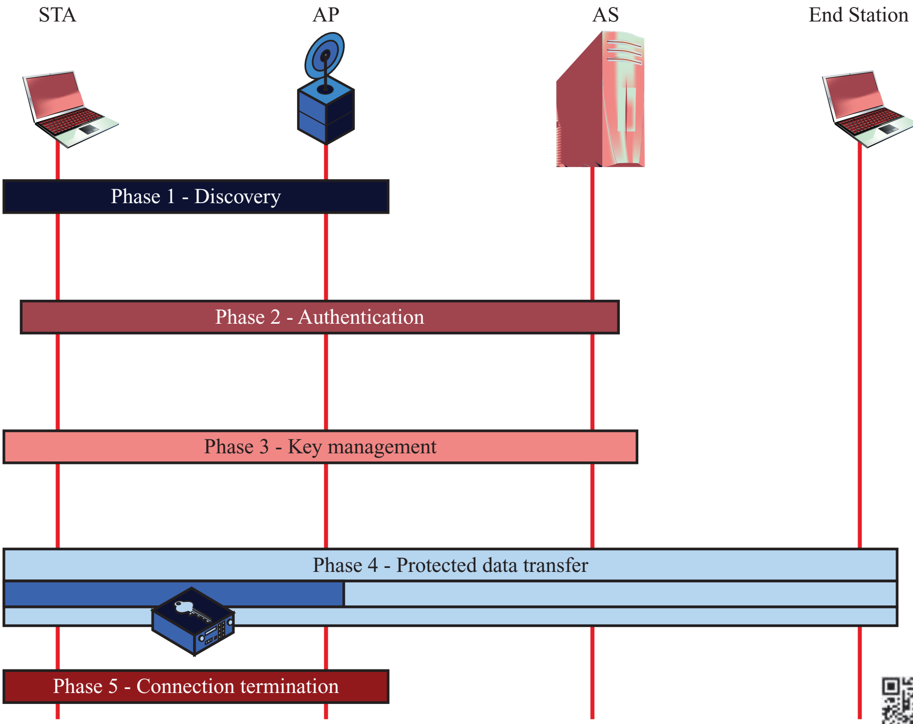


Figure 11.21 IEEE 802.11i Phases of Operation

2. Two wireless stations (STAs) in the same ad hoc IBSS communicating directly with each other.
3. Two wireless stations in different BSSs communicating via their respective APs across a distribution system.
4. A wireless station communicating with an end station on a wired network via its AP and the distribution system.

IEEE 802.11i security is concerned only with secure communication between the STA and its AP. In case 1 in the preceding list, secure communication is assured if each STA establishes secure communications with the AP. Case 2 is similar, with the AP functionality residing in the STA. For case 3, security is not provided across the distribution system at the level of IEEE 802.11, but only within each BSS. End-to-end security (if required) must be provided at a higher layer. Similarly, in case 4, security is only provided between the STA and its AP.

With these considerations in mind, Figure 11.21 depicts the five phases of operation for an RSN and maps them to the network components involved. One new component is the AS. The rectangles indicate the exchange of sequences of MPDUs. The five phases are defined as follows:

- **Discovery:** An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.

- **Authentication:** During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.
- **Key generation and distribution:** The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only.
- **Protected data transfer:** Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.
- **Connection termination:** The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.

Discovery Phase We now look in more detail at the RSN phases of operation, beginning with the discovery phase. The purpose of this phase is for an STA and an AP to recognize each other, agree on a set of security capabilities, and establish an association for future communication using those security capabilities.

The discovery phase consists of three exchanges.

- **Network and security capability discovery:** During this exchange, STAs discover the existence of a network with which to communicate. The AP either periodically broadcasts its security, indicated by RSN IE (Robust Security Network Information Element), in a specific channel through the Beacon frame, or it responds to a station's Probe Request through a Probe Response frame. A wireless station may discover available access points and corresponding security capabilities by either passively monitoring the Beacon frames or actively probing every channel.
- **Open system authentication:** The purpose of this frame sequence, which provides no security, is simply to maintain backward compatibility with the IEEE 802.11 state machine, as implemented in existing IEEE 802.11 hardware. In essence, the two devices (STA and AP) simply exchange identifiers.
- **Association:** The purpose of this stage is to agree on a set of security capabilities to be used. The STA then sends an Association Request frame to the AP. In this frame, the STA specifies one set of matching capabilities from among those advertised by the AP. If there is no match in capabilities between the AP and the STA, the AP refuses the Association Request. The STA blocks it too, in case it has associated with a rogue AP or someone is inserting frames illicitly on its channel.

Authentication Phase As was mentioned, the authentication phase enables mutual authentication between an STA and an AS located in the DS. Authentication is designed to allow only authorized stations to use the network and to provide the STA with assurance that it is communicating with a legitimate network.

IEEE 802.11i makes use of another standard that was designed to provide access control functions for LANs. The standard is IEEE 802.1X, Port-Based Network Access Control. The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard. IEEE 802.1X uses the terms *supplicant*, *authenticator*, and *authentication server*. In the context of an 802.11 WLAN, the first two terms correspond to the wireless station and the AP. The AS is typically a separate device on the wired side of the network (i.e., accessible over the DS) but could also reside directly on the authenticator.

Before the AS authenticates a supplicant using an authentication protocol, the authenticator only passes control or authentication messages between the supplicant and the AS; the 802.1X control channel is unblocked, but the 802.11 data channel is blocked. Once a supplicant is authenticated and keys are provided, the authenticator can forward data from the supplicant, subject to predefined access control limitations for the supplicant to the network. Under these circumstances, the data channel is unblocked.

We can think of authentication phase as consisting of the following three phases:

- **Connect to AS:** The STA sends a request to its AP (the one with which it has an association) for connection to the AS. The AP acknowledges this request and sends an access request to the AS.
- **EAP exchange:** This exchange authenticates the STA and AS to each other. A number of alternative exchanges are possible.
- **Secure key delivery:** Once authentication is established, the AS generates a master session key (MSK), also known as the Authentication, Authorization, and Accounting (AAA) key, and sends it to the STA. All the cryptographic keys needed by the STA for secure communication with its AP are generated from this MSK. IEEE 802.11i does not prescribe a method for secure delivery of the MSK but relies on EAP for this. Whatever method is used, it involves the transmission of an MPDU containing an encrypted MSK from the AS, via the AP, to the STA.

Key Management Phase During the key management phase, a variety of cryptographic keys are generated and distributed to STAs. There are two types of keys: pairwise keys used for communication between an STA and an AP and group keys used for multicast communication. Discussion of these keys is provided in [STAL13b].

Protected Data Transfer Phase IEEE 802.11i defines two schemes for protecting data transmitted in 802.11 MPDUs: the **Temporal Key Integrity Protocol (TKIP)** and the **Counter Mode-CBC MAC Protocol (CCMP)**.

TKIP TKIP is designed to require only software changes to devices that are implemented with the older wireless LAN security approach called wired equivalent privacy. TKIP provides two services:

- **Message integrity:** TKIP adds a message integrity code (MIC) to the 802.11 MAC frame after the data field. The MIC is generated by an algorithm, called Michael, which computes a 64-bit value using as input the source and destination MAC address values and the Data field, plus key material.
- **Data confidentiality:** Data confidentiality is provided by encrypting the MPDU plus MIC value using the RC4 encryption algorithm.

CCMP CCMP is intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme. As with TKIP, CCMP provides two services:

- **Message integrity:** CCMP uses the cipher-block-chaining message authentication code (CBC-MAC).
- **Data confidentiality:** CCMP uses the CTR block cipher mode of operation and the AES algorithm for encryption. The same 128-bit AES key is used for both integrity and confidentiality.

11.9 RECOMMENDED READING

A brief but useful survey of 802.11 is [MCFA03]. [GEIE01] has a good discussion of OFDM in IEEE 802.11a. [CISC07] and [PERA08] are technical treatments of IEEE 802.11n. [HALP10] and [PAUL08] examine the 802.11n MIMO scheme. [ALSA13], [CISC14], and [VERM13] are good technical introductions to 802.11ac. [CORD10] and [PERA10] provide good technical overviews of 802.11ad. [HIER10] summarizes all 802.11 activity, and [XIAO04] discusses 802.11e. [STAL13] provides a thorough treatment of 802.11i security.

ALSA13 Alsabbagh, E.; Yu, H.; and Gallagher, K. “802.11ac Design Consideration for Mobile Devices.” *Microwave Journal,* February 2013.

CISC07 Cisco Systems, Inc. “802.11n: The Next Generation of Wireless Performance.” Cisco White Paper, 2007. cisco.com

CORD10 Cordeiro, C.; Akhmetov, D.; and Park, M. “IEEE 802.11ad: Introduction and Performance Evaluation of the First Multi-Gbps Wi-Fi Technology.” *Proceedings of the 2010 ACM international workshop on mmWave communications: from circuits to networks,* 2010.

GEIE01 Geier, J. “Enabling Fast Wireless Networks with OFDM.” *Communications System Design,* February 2001.

HALP10 Halperin, D., et al. “802.11 with Multiple Antennas for Dummies.” *Computer Communication Review,* January 2010.

HIER10 Hiertz, G.R.; Denteneer, D.; Stibor, L.; Zang, Y.; Costa, X.P.; and Walke, B. “The IEEE 802.11 universe.” *Communications Magazine, IEEE,* vol. 48, no. 1, pp. 62, 70, January 2010.

MCFA03 McFarland, B., and Wong, M. “The Family Dynamics of 802.11.” *ACM Queue,* May 2003.

PAUL08 Paul, T., and Ogunfunmi, T. “Wireless LAN Comes of Age: Understanding the IEEE 802.11n Amendment.” *Circuits and Systems Magazine, IEEE,* vol. 8, no. 1, pp. 28, 54, First Quarter 2008.

PERA08 Perahia, E. "IEEE 802.11n Development: History, Process, and Technology." Communications Magazine, IEEE, vol. 46, no. 7, pp. 48, 55, July 2008.

PERA10 Perahia, E., et al. "IEEE 802.11ad: Defining the Next Generation Multi-Gbps Wi-Fi." *Proceedings, 7th IEEE Consumer Communications and Networking Conference,* 2010.

STAL13 Stallings, W. *Cryptography and Network Security: Principles and Practice, Sixth Edition.* Upper Saddle *River*, NJ: Prentice Hall, 2013.

VERM13 Verma, L.; Fakharzadeh, M.; and Sunghyun Choi. "Wi-Fi on steroids: 802.11AC and 802.11AD." *Wireless Communications, IEEE,* vol. 20, no. 6, pp. 30, 35, December 2013.

XIAO04 Xiao, Y. "IEEE 802.11e: QoS Provisioning at the MAC Layer." *IEEE Communications Magazine,* June 2004.

11.10 KEY TERMS, REVIEW QUESTIONS, AND PROBLEMS

Key Terms

access point (AP)

ad hoc networking

authentication server (AS)

basic service set (BSS)

binary exponential backoff

complementary code keying (CCK)

counter mode-CBC MAC protocol (CCMP)

distributed coordination function (DCF)

distribution system (DS)

extended service set (ESS)

independent BSS (IBSS)

Kiviat graph

logical link control (LLC)

MAC protocol data unit (MPDU)

MAC service data units (MSDUs)

medium access control (MAC)

open system authentication

point coordination function (PCF)

service set identifier (SSID)

spread spectrum wireless LAN

Temporal Key Integrity Protocol (TKIP)

wired equivalent privacy (WEP)

Wi-Fi

Wi-Fi protected access (WPA)

wireless LAN (WLAN)

Review Questions

11.1 List and briefly define the IEEE 802 protocol layers.

11.2 What is a Kiviat graph?

11.3 What is the difference between a MAC address and an LLC address?

11.4 Is a distribution system a wireless network? Why or why not?

11.5 List and briefly define IEEE 802.11 services.

11.6 How is the concept of an association related to that of mobility?

11.7 What is the difference between a single-cell and a multiple-cell WLAN?

11.8 What characteristics of a wireless LAN present unique security challenges not found in wired LANs?

11.9 On the Wi-Fi Alliance Web site (www.wi-fi.org), investigate Wi-Fi Direct technology. How is this technology useful? What features does it add to the base 802.11 ad hoc WLAN functionality illustrated in Figure 11.3?

Problems

11.1 Answer the following questions about your wireless network:

a. What is the SSID?

b. Who is the equipment vendor?

c. What standard are you using?

d. What is the size of the network?

11.2 For IEEE 802.11n, determine the data rate for 16 QAM using a 2/3 coding rate with 2 parallel data streams.

a. For a 20 MHz channel.

b. For a 40 MHz channel.

11.3 For IEEE 802.11ac, determine the data rate over a 160 MHz channel for 64 QAM using a 1/2 coding rate with 8 parallel data streams.

11.4 There are many free tools and applications available for helping decipher wireless networks. One of the most popular is Netstumbler. Obtain the software at www.netstumbler.com and follow the links for downloads. The site has a list of supported wireless cards. Using the Netstumbler software, determine the following:

a. How many access points in your network have the same SSID?

b. What is your signal strength to your access point?

c. How many other wireless networks and access points can you find?

11.5 Most wireless cards come with a small set of applications that can perform tasks similar to Netstumbler. Using your own client software, determine the same items you did with Netstumbler. Do they agree?

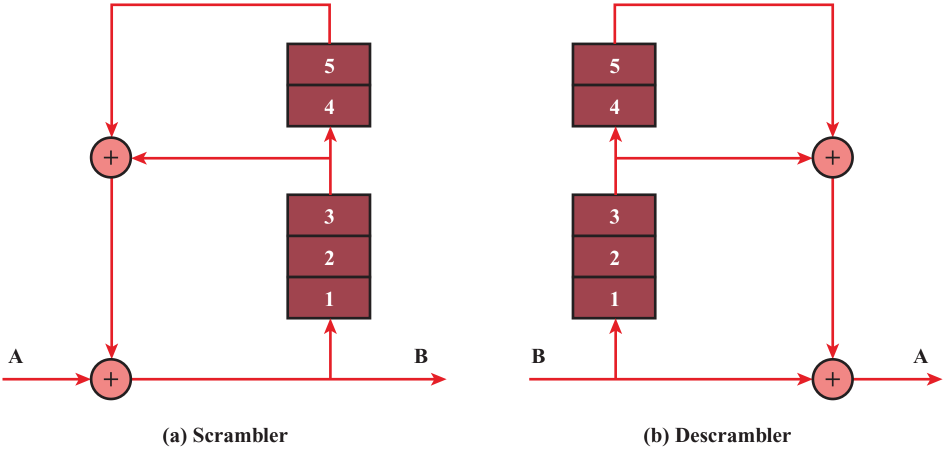
11.6 Try this experiment: How far can you go in different directions and still be connected to your network? This will depend to a large extent on your physical environment.

11.7 Compare and contrast wired and wireless LANs. What unique concerns must be addressed by the designer of a wireless LAN network?

11.8 For the 802.11 scrambler and descrambler described in Appendix 11A,

a. Show the expression with exclusive-or operators that corresponds to the polynomial definition.

b. Draw a figure similar to Figure 11.22.



(a) Scrambler

(b) Descrambler

Figure 11.22 Scrambler and Descrambler

APPENDIX 11A SCRAMBLING

For some digital data encoding techniques, a long string of binary zeros or ones in a transmission can degrade system performance. Also, other transmission properties, such as spectral properties, are enhanced if the data are more nearly of a random nature rather than constant or repetitive. A technique commonly used to improve signal quality is scrambling and descrambling. The scrambling process tends to make the data appear more random.

The scrambling process consists of a feedback shift register, and the matching descrambler consists of a feedforward shift register. An example is shown in Figure 11.22. In this example, the scrambled data sequence may be expressed as follows:

$$B_m = A_m \oplus B_{m-3} \oplus B_{m-5}$$

where $\oplus$ indicates the exclusive-or operation. The descrambled sequence is

$$\begin{aligned} C_m &= B_m \oplus B_{m-3} \oplus B_{m-5} \\ &= (A_m \oplus B_{m-3} \oplus B_{m-5}) \oplus B_{m-3} \oplus B_{m-5} \\ &= A_m (\oplus B_{m-3} \oplus B_{m-3}) \oplus (B_{m-5} \oplus B_{m-5}) \\ &= A_m \end{aligned}$$

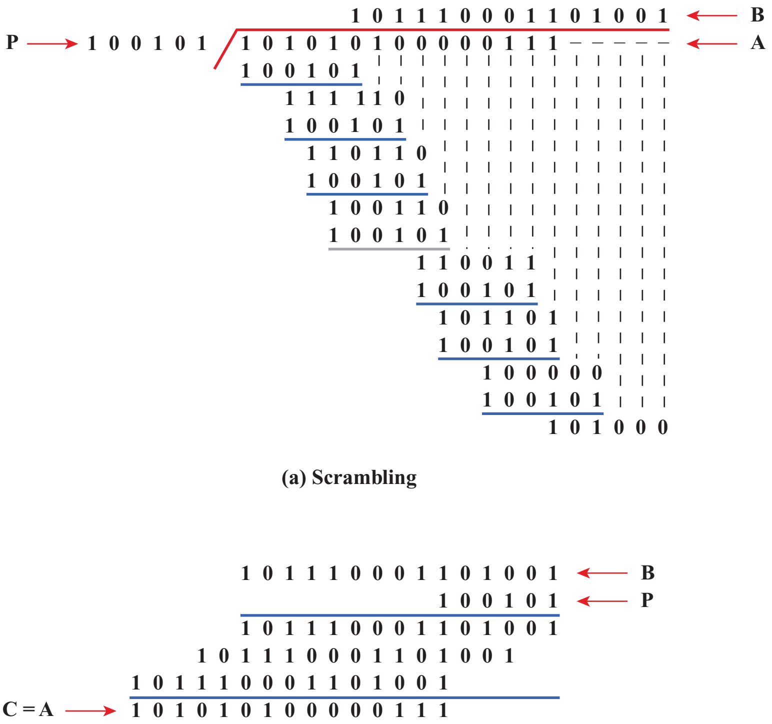
As can be seen, the descrambled output is the original sequence.

We can represent this process with the use of polynomials. Thus, for this example, the polynomial is $P(X) = 1 + X^3 + X^5$. The input is divided by this polynomial to produce the scrambled sequence. At the receiver, the received scrambled signal is multiplied by the same polynomial to reproduce the original input. Figure 11.23 is an example using the polynomial $P(X)$ and an input of 101010100000111. The scrambled transmission, produced by dividing by $P(X)$ (100101), is 101110001101001. When this number is multiplied by $P(X)$, we get the original input. Note that the input sequence contains the periodic sequence 10101010 as well as a long string of zeros. The scrambler effectively removes both patterns.

For 802.11, the scrambling equation is

$$P(X) = 1 + X^4 + X^7$$

In this case, the shift register consists of seven elements, used in the same manner as the five-element register in Figure 11.22.



(a) Scrambling

(b) Descrambling

Figure 11.23 Example of Scrambling with $P(X) = 1 + X^{-3} + X^{-5}$