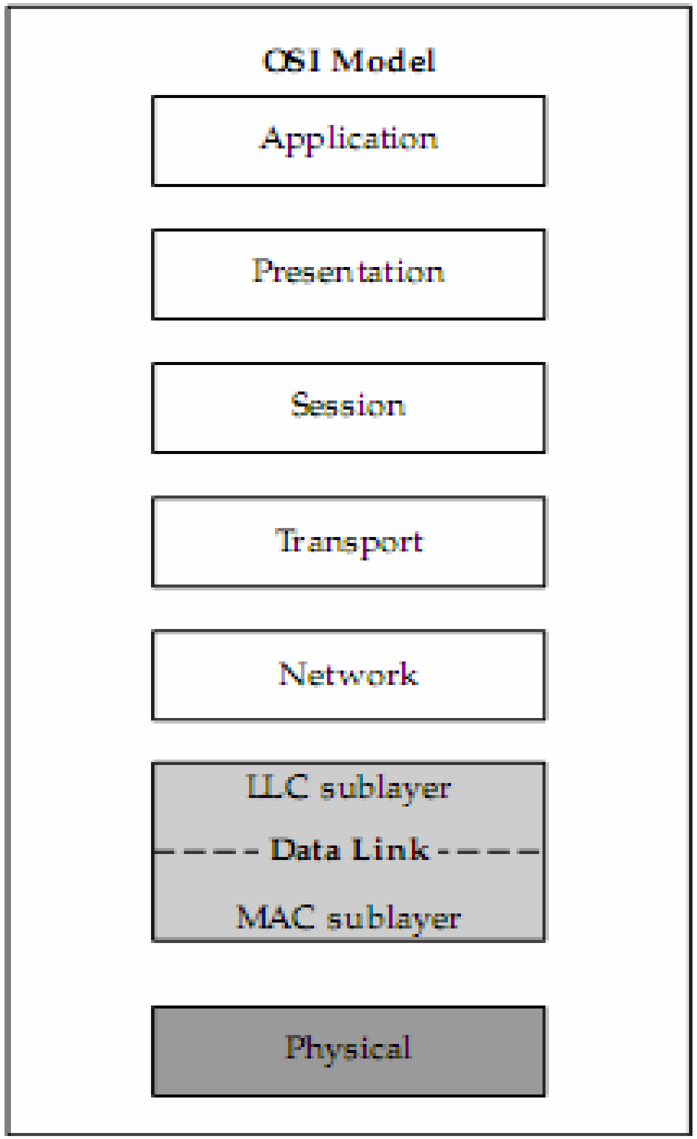
HW

Institute of Electrical and Electronics Engineers (IEEE)

IEEE 802.11 standard**s**

WLAN Standard (IEEE 802.11)

- The IEEE 802.11 is a family of standards that governs the operations and functions of WLANs. But the standard does not define or manage absolutely every aspect of WLAN operations—it specifically concerns itself only with the functions of WLANs at the Physical (PHY) layer and Media Access Control sublayer of the OSI reference model. The following figure shows the entire OSI model.



OSI reference model

Physical layer

- The Physical layer is the first layer (Layer 1) in the OSI reference model. It defines the relationship between a device and the physical communication *medium*.
- The IEEE 802.11 of Physical layer specifies the *wireless signaling techniques* used for transmitting and receiving information over the airwaves. Some sample signaling techniques are listed below:

Frequency-hopping spread spectrum (FHSS)

This signaling (modulation) technique specifies use in the 2.4 GHz industrial, scientific, and medical (ISM) frequency band. The specific frequency range is 2.402–2.480 GHz. FHSS is one of the modulation techniques used in early WLAN implementations and is rarely used today. It supports data rates of 1–2 Mbit/s.

Direct-sequence spread spectrum (DSSS)

- This signaling (modulation) technique specifies use in the 2.4 GHz ISM band. The specific frequency range is 2.400–2.497 GHz. Systems implementing this PHY can support 1 Mbit/s and 2 Mbit/s data rates.
- **High rate direct sequence spread spectrum (HR/DSSS)**

Systems implementing this PHY can provide data rates of 1, 2, 5.5, and 11 Mbit/s.

Orthogonal frequency division multiplexing (OFDM)

Specifies use in the 5 GHz frequency bands and the 2.4 GHz ISM bands. Most of the recent IEEE 802.11 standards implement this PHY and its variants. OFDM generally supports higher data rates. Systems implementing this PHY can support 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s data rates.

MAC

- To maintain some safety in data communications, certain rules and guidelines must be established and followed. This is especially important in wireless communications because of the nature of the medium used for the communications—air or space. The rules and guidelines are specified at different layers of the OSI model.

MAC is a sublayer of the OSI’s Data Link layer, or layer 2. The MAC sublayer is basically responsible for providing addressing and medium access control mechanisms that make it possible for several nodes to communicate in a network. The MAC functions are used to control and manage access to the transmission medium in a communications system.

- Controlling the access of stations plugged into a wired Ethernet LAN (IEEE 802.3) is relatively simple because of the use of cables. All nodes plugged into the same network can easily sense the presence or absence of an electric current in their cables. The electric current here implies the data transmission. To coordinate access to the LAN medium, LAN stations use Carrier Sense Multiple Access with Collision Detection (CSMA/CD). The key word here is “detection.”

The rules that govern the IEEE 802.11 WLANs can not easily use same method for managing access to the shared medium used in wired LANs. And there are several reasons behind this—one reason is the absence of physical wires.

- The STAs in a wireless network cannot always be guaranteed to be within earshot of each other so that they can hear (or detect) when the other STAs are transmitting. This phenomena is known as the “*hidden node*” problem in RF communications. Furthermore, the transmission may not even be destined for the hidden node, but it still needs to use the common transmission medium shared by all the nodes.

- The second reason is because the radio in most wireless LAN hardware is capable of operating in either a transmitting or receiving mode at one time—it can’t usually do both at the same time. For the wireless hardware to be able to detect collisions (receive mode) while it is sending data (transmit mode), it needs to include a radio that offers such capabilities. And as has already been mentioned, this is not the case in wireless LAN hardware.

- So instead of attempting to detect when the medium is available for use, 802.11based systems take a different way by trying to avoid any type of collision in the first place. This is *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)*, and the key word here is “avoidance.”

A popular method for implementing CSMA/CA in wireless LANs is known as the Distributed Coordination Function (DCF). The following steps show how three sample wireless STAs (STA-a, STA-b, and STA-c) might negotiate access to the wireless medium. Note that this is only one of the several methods by which CSMA/CA can be implemented.

1. STA-a needs to access the wireless medium, so it puts its radio in receiving mode to see if any other STAs are currently transmitting anything.
2. If STA-a sees that the medium is in use by STA-b, it waits until STA-b is done with its transmission. The amount of time that STA-a waits is determinate.
3. STA-a will attempt to transmit again by first checking to see if the medium is available. If so, STA-a will send out a special MAC frame called a Request To Send (RTS) frame. Also called a control frame, this is one of several MAC frame types (as discussed in the next section).
4. STA-c will see the special frame sent from STA-a and in turn send a Clear To Send (CTS) frame. STA-a will send its message to STA-c.
5. For the communication to be considered successful, STA-c needs to send an acknowledgement confirming that it indeed received the message sent by STA-a. This message is carried in another control frame type called an Acknowledgment (ACK) frame. This is also known as positive acknowledgement.
6. If, for whatever reason, STA-a does not receive an ACK message from STA-c, it resends the message.

MAC Frame Types

- Depending on their function, IEEE 802.11 MAC frame types can be grouped into three categories: *control frames*, *management frames*, and *data frames*.

Control Frames

These most basic frame types are very important for all WLAN communications and are used to support the delivery of the other (management and data) MAC frame types. All the wireless STAs must be able to see the control frames—in other words, the information in the control frames is not secret or classified in any way.

Control frames are used, for example, when a wireless STA needs to negotiate and gain access to the WLAN using CSMA/CA. Other types of control frames are the Request to Send (RTS), Clear to Send (CTS), and Acknowledgment (ACK) frames.

Management Frames

These frame types are used for management purposes on the WLAN, where they play a very important role. Management frames are used by wireless STAs whenever an STA officially wants to participate or discontinue its participation in the network and for other miscellaneous housekeeping purposes. Here are some sample management frame types:

- **Beacon frame** A very important management MAC frame type, it performs various functions, such as time synchronization among the STAs; it also stores the value of the SSID being used, and specifies the data rates supported on the WLAN, among other things.
- **Association Request frame** These frames are sent by the STA to request association with the AP.
- **Association Response frame** These frames contains the AP's response to the STA regarding the STA's association request. It is either a yeas or no.
- **Reassociation Request frame** These frames are used by STAs whenever they need to be reassociated with an AP.
- **Reassociation Response frame** These frames are sent by the AP in response to the STAs request to reassociate with the AP

- ■ **Authentication frame** These frames are used whenever a STA needs to participate in or join a BSS. Mere association is not nearly enough—the STA needs to be authenticated to make full use of the BSS. The STA uses authentication frame types to confirm its identity.
- ■ **Deauthentication frame** Authenticated STAs use these frame types to signal their intention to terminate the authenticated (secure) communications.
- ■ **Disassociation frame** This frame is sent by a STA that is associated with an AP to inform the AP that it wants to discontinue the association. Note that this is not a request, and as such a response or acknowledgment or confirmation is not required from the AP.
- ■ **Probe Request frame** STAs send probe request frames whenever they need to discover information about other STAs. Such information might include the capabilities of the other STA or information about the supported data rates.
- ■ **Probe Response frame** This frame carries the response to probe requests.

Data Frames

These frame types are responsible for transporting the actual data payload to and from the communication end points.

Reference

Wale soyinka, **Wireless Network Administration A Beginner’s Guide**, The McGraw-Hill Companies , 2010.