3.1 To Understand Wireless LAN Technology

3.1.1 Distinguish Single cell and multiple cell wireless LAN configurations

Wireless LAN

- A wireless LAN uses wireless transmission medium
- Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN.
- Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

Wireless LAN Applications

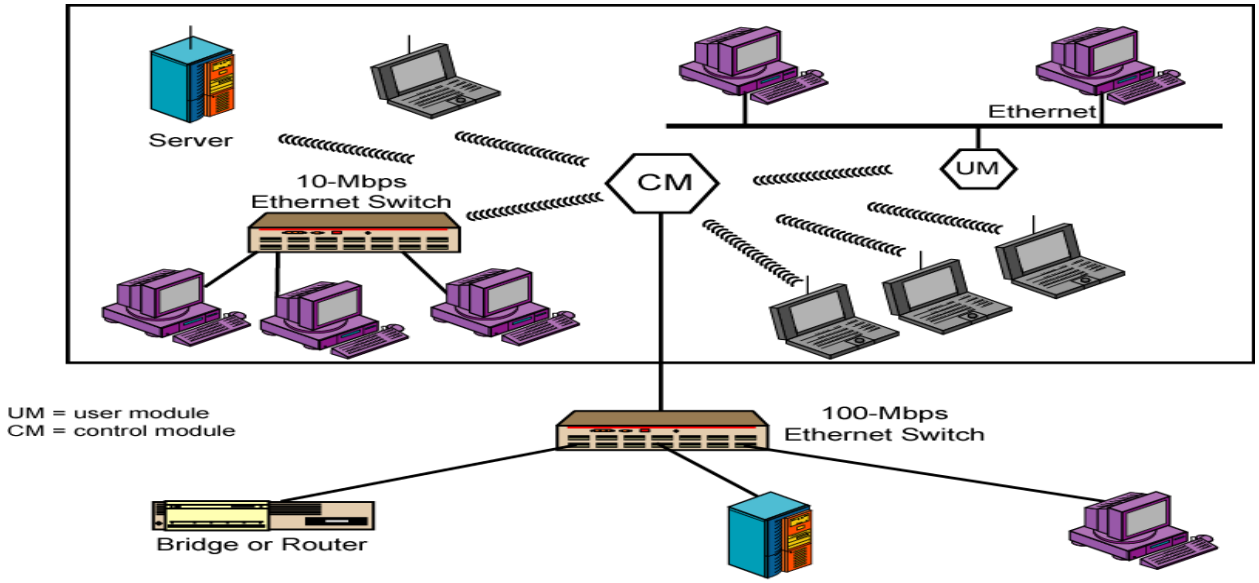
Four application areas for wireless LANs:

1.LAN extension
2. Crossbuilding interconnect,
3. Nomadic access
4. ad hoc networks.

1. **LAN Extension**:-
   - Saves cost of installation of LAN cabling
   - Eases relocation and other modifications to network structure

- For example, a manufacturing facility typically has an office area that is separate from the factory floor but that must be linked to it for networking purposes.
- Therefore, typically, a wireless LAN will be linked into a wired LAN on the same premises. Thus, this application area is referred to as LAN extension

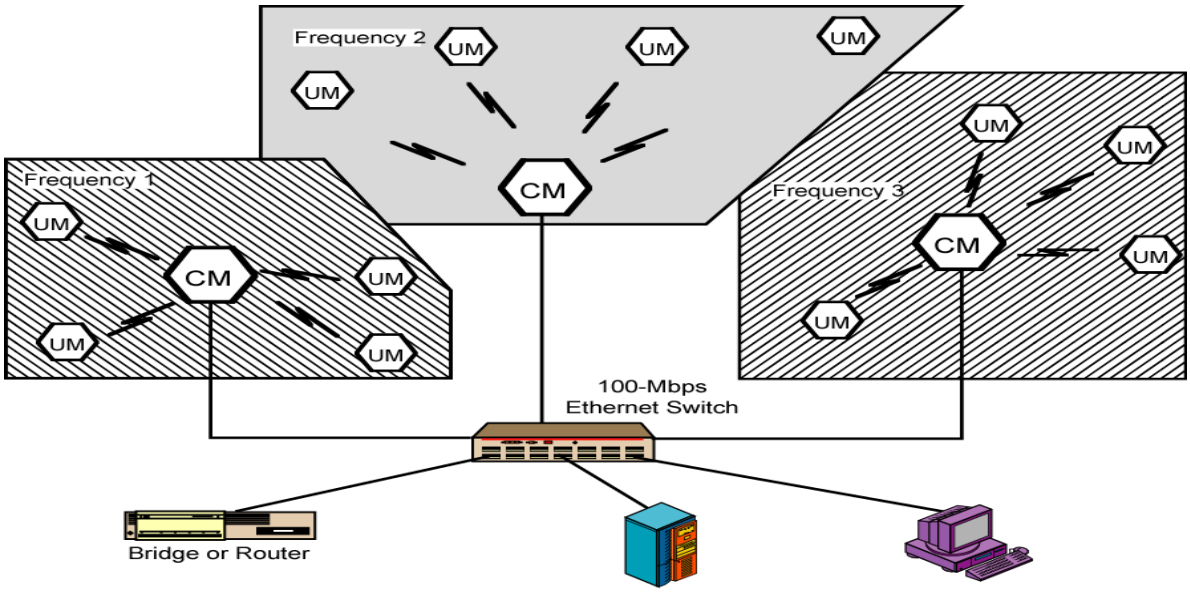
Single cell wireless LAN configuration



- 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
- 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 can be referred to as a single-cell wireless LAN; all of the wireless end systems are within range of a single control module.

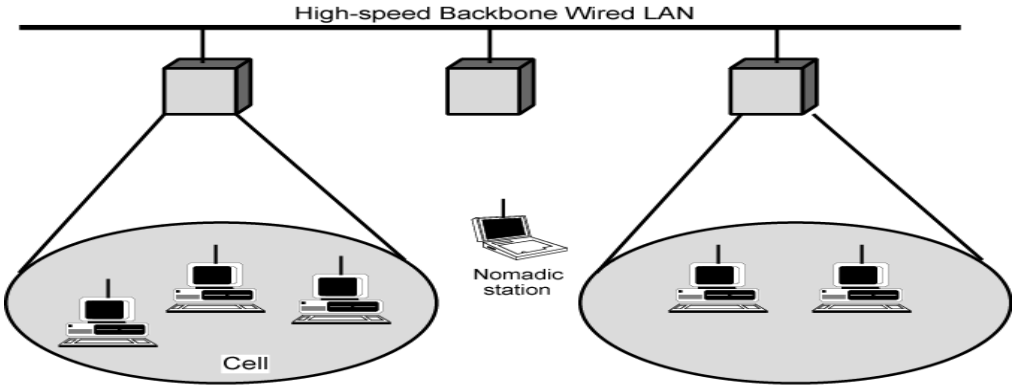
Multiple-cell wireless LAN



- Another common configuration, suggested by Figure above, 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 an infrared LAN, transmission is limited to a single room; therefore, one cell is needed for each room in an office building that requires wireless support.

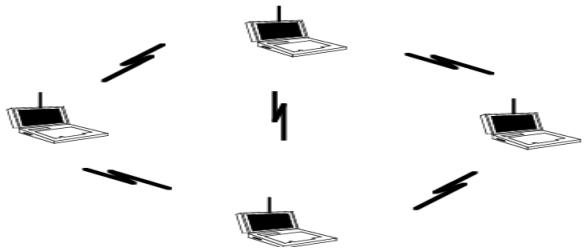
2. **Cross-Building Interconnect**:-
   - Another use of wireless LAN technology is to connect LANs in nearby buildings, be they wired or wireless LANs.
   - In this case, a point-to-point wireless link is used between two buildings.
   - The devices so connected are typically bridges or routers.
   - This single point-to-point link is not a LAN perse, but it is usual to include this application under the heading of wireless LAN.
3. **Nomadic Access**:-
   - Nomadic access provides a wireless link between a LAN hub and a mobile data terminal equipped with an antenna, such as a laptop computer or notepad computer.
   - One example of the utility of such a connection is to enable an employee returning from a trip to transfer data from a personal portable computer to a server in the office.

- Nomadic access is also useful in an extended environment such as a campus or a business operating out of a cluster of buildings.
- In both of these cases, users may move around with their portable computers and may wish access to the servers on a wired LAN from various locations.
- Nomadic stations can move from one cell to another.



(a) Infrastructure Wireless LAN

4. **Ad Hoc Networking** :-



- 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 employees, each with a laptop or palmtop computer, may convene in a conference room for a business or classroom meeting.
- The employees link their computers in a temporary network just for the duration of the meeting
- No infrastructure for an ad hoc network.
- The stations may dynamically configure themselves into a temporary network.

3.1.2 Discuss requirements of wireless LAN

- ❖ A wireless LAN requirement is same as that of any LAN including:
  - High capacity
  - Coverage distance
  - Connectivity among stations
  - Broadcast capability.
- ❖ In addition, the most important requirements for wireless LANs:

• **Throughput:** The medium access control protocol should make as efficient use as possible of the wireless medium to maximize capacity.
• **Number of nodes:** Wireless LANs 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 wireless LANs, 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 and ad hoc wireless networks.

• **Service area:** A typical coverage area for a wireless LAN has a diameter of 100 to 300 m.

• **Battery power consumption**: Mobile workers use battery-powered workstations that need to have a long battery life when used with wireless adapters. 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 wireless LAN implementations have features to reduce power consumption while not using the network, such as a sleep mode.

• **Transmission robustness and security:** Unless properly designed, a wireless LAN may be interference prone and easily eavesdropped. The design of a wireless LAN must permit reliable transmission even in a noisy environment and should provide some level of security from eavesdropping.

• **Collocated network operation**: As wireless LANs become more popular, it is quite likely for two or more wireless LANs to operate in the same area or in some area where interference between the LANs is possible. Such interference may thwart the normal operation of a MAC algorithm and may allow unauthorized access to a particular LAN.

• **License-free operation:** Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.

• **Hand-offroaming:** The MAC protocol used in the wireless LAN should enable mobile stations to move from one cell to another.

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

WLAN Categories

Wireless LANs are generally categorized according to the transmission technique that is used. All current wireless LAN products fall into one of the following categories:

• **Infrared (lR) LANs:** An individual cell of an IR LAN is limited to a single room, because infrared light does not penetrate opaque walls.

• **Spread spectrum LANs:** This type of LAN makes use of spread spectrum transmission technology. In most cases, these LANs operate in the ISM (Industrial, Scientific, and Medical) bands so that no FCC licensing is required for their use in the United States.

• **Narrowband microwave:** These LANs operate at microwave frequencies but do not use spread spectrum. Some of these products operate at frequencies that require FCC licensing, while others use one of the unlicensed ISM bands.

Table 13.1 Comparison of Wireless LAN Technologies

	Infrared		Spread Spectrum		Radio
	Diffused Infrared	Directed Beam Infrared	Frequency Hopping	Direct Sequence	Narrowband Microwave
Data Rate (Mbps)	1 to 4	1 to 10	1 to 3	2 to 54	10 to 20
Mobility	Stationary/mobile	Stationary with LOS	Mobile	Stationary/mobile	
Range (m)	15 to 60	25	30 to 100	30 to 250	10 to 40
Detectability	Negligible		Little		Some
Wavelength/ frequency	λ: 800 to 900 nm		902 to 928 MHz 2.4 to 2.4835 GHz 5.725 to 5.85 GHz		902 to 928 MHz 5.2 to 5.775 GHz 18.825 to 19.205 GHz
Modulation technique	ASK		FSK	QPSK	FS/QPSK
Radiated power	—		<1 W		25 mW
Access method	CSMA	Token Ring, CSMA	CSMA		Reservation ALOHA, CSMA
License required	No		No		Yes unless ISM

3.1.3 Describe Infrared LAN

- ❖ Optical wireless communication in the infrared portion of the spectrum is commonplace in most homes, where it is used for a variety of remote control devices.
- ❖ More recently, attention has turned to the use of infrared technology to construct wireless LANs.

A comparison of the characteristics of infrared LANs with those of radio LANs

IR LAN Strengths

- The two competing transmission media for wireless LANs are microwave radio, using either spread spectrum or narrowband transmission, and infrared.
- Infrared offers a number of significant advantages over the microwave radio approaches.
    a) First, the spectrum for infrared is virtually unlimited, which presents the possibility of achieving extremely **high data rates**.
    b) The infrared spectrum is unregulated worldwide, which is not true of some portions of the microwave spectrum.
    c) In addition, infrared shares some properties of visible light that make it attractive for certain types of LAN configurations.
    d) Infrared light is diffusely reflected by light-colored objects; thus it is possible to use ceiling reflection to achieve coverage of an entire room.
    e) Infrared light does not penetrate walls or other opaque objects.
    f) This has two advantages:
        - First, infrared communications can be more easily secured against eavesdropping than microwave;
        - Second, a separate infrared installation can be operated in every room in a building without interference, enabling the construction of very large infrared LANs.
    g) The equipment is relatively **inexpensive and simple**.
    h) Infrared data transmission typically uses intensity modulation, so that IR receivers need to detect only the amplitude of optical signals, whereas most microwave receivers must detect frequency or phase.

IR LAN Weaknesses

The infrared medium also exhibits some drawbacks-

- Many indoor environments experience rather intense infrared background radiation, from sunlight and indoor lighting.
- This radiation appears as noise in an IR receiver requiring higher power and limiting range.
- increases in transmitter power are limited by eye safety and excessive power consumption

IR LAN- Transmission Techniques

- There are three alternative transmission techniques commonly used for IR data transmission:
  1. The transmitted signal can be focused and aimed (as in a remote TV control)
  2. It can be radiated omnidirectionally
  3. It can be reflected from a light-colored ceiling.

1. Directed Beam Infrared

- Directed beam IR can be used to create point-to-point links. In this mode, the range depends on the emitted power and on the degree of focusing.
- A focused IR data link can have a range of kilometers. Such ranges are not needed for constructing indoor wireless LANs.
- However, an IR link can be used for cross-building interconnect between bridges or routers located in buildings within a line of sight of each other.
- One indoor use of point-to-point IR links is to set up a token ring LAN (Figure).
- A set of IR transceivers can be positioned so that data circulate around them in a ring configuration.
- Each transceiver supports a workstation or a hub of stations, with the hub providing a bridging function.

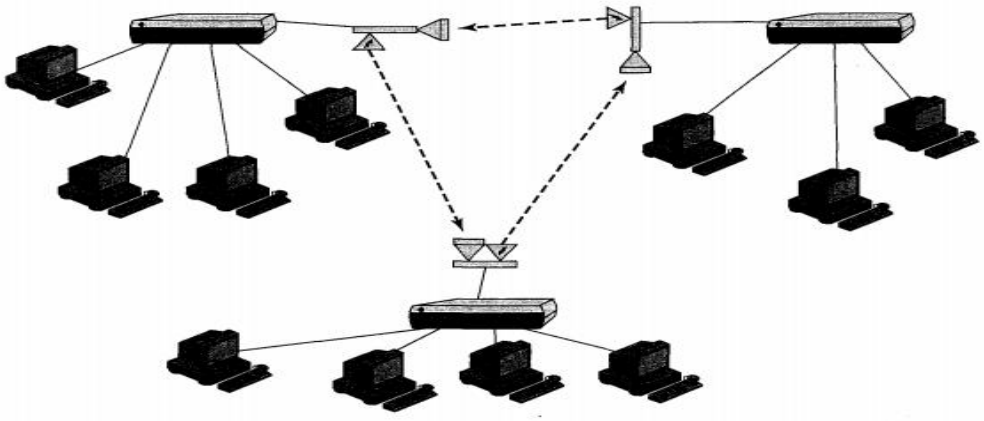


Figure 13.5 Token Ring LAN Using Point-to-Point Infrared Links

2. Omnidirectional

- An omnidirectional configuration involves a single base station that is within line of sight of all other stations on the LAN.
- Typically, this station is mounted on the ceiling (Figure 13.6a).
- The base station acts as a multiport repeater.
- The ceiling transmitter broadcasts an omnidirectional signal that can be received by all of the other IR transceivers in the area.
- These other transceivers transmit a directional beam aimed at the ceiling base unit.

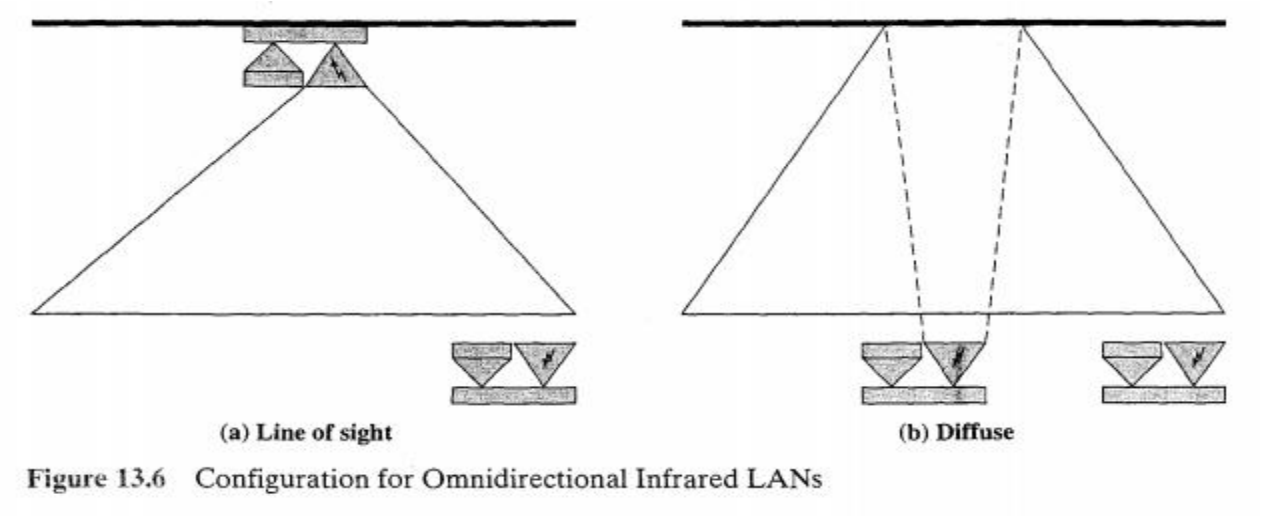


Figure 13.6 Configuration for Omnidirectional Infrared LANs

3. Diffused

- In this configuration, all of the IR transmitters are focused and aimed at a point on a diffusely reflecting ceiling (Figure 13.6b).
- IR radiation striking the ceiling is reradiated omnidirectionally and picked up by all of the receivers in the area.
- Figure 13.7 shows a typical configuration for a wireless IR LAN installation.
- There are a number of ceiling-mounted base stations, one to a room. Each station provides connectivity for a number of stationary and mobile workstations in its area.
- Using ceiling wiring, the base stations are all connected back to a server that can act as an access point to a wired LAN or a WAN. In addition, there may be conference rooms without a base station where ad hoc networks may be set up.

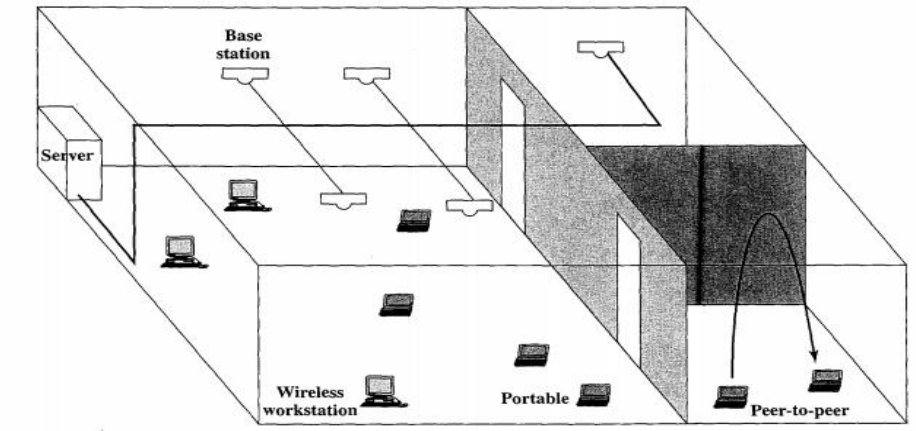


Figure 13.7 Network of Portable and Stationary Wireless Stations Using Infrared

3.1.4 Describe Spread Spectrum LAN

The most popular type of wireless LAN uses spread spectrum techniques.

Configuration

- Except for quite small offices, a spread spectrum wireless LAN makes use of a multiple-cell arrangement
- 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.
- In hub topology, the hub is mounted on the ceiling

- Connected to a wired LAN
- Connected to stations attached to the wired LAN and to stations that are part of wireless LANs
- The hub also controls access. Also acts as a multiport repeater
- All stations in the cell transmit to the hub and receive from the hub.
- Station may broadcast using an omnidirectional antenna.
- Hub does automatic handoff of mobile stations.
- 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 CSMA is used to control access. This topology is appropriate for ad hoc LANs.

Transmission Issues

- A desirable, though not 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 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 has become popular.
- In the United States, three microwave bands have been set aside for unlicensed spread spectrum use: 902-928 MHz (915 MHz band), 2.4-2.4835 GHz (2.4 GHz band), and 5.725-5.825 GHz (5.8 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 three 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 little competition at the 5.8 GHz band; however, the higher the frequency band, in general the more expensive the equipment.
- Until recently, typical spread spectrum wireless LANs were limited to just 1 to 3 Mbps.

3.1.5 Describe Narrowband Microwave LAN

❖ The term narrowband microwave refers to the use of a microwave radio frequency band for signal transmission, with a relatively narrow bandwidth-just wide enough to accommodate the signal.

❖ Until recently, all narrowband microwave LAN products have used a licensed microwave band.

❖ More recently, at least one vendor has produced a LAN product in the ISM band.

➔ Licensed Narrowband RF

✓ Microwave radio frequencies usable for voice, data, and video transmission are licensed and coordinated within specific geographic areas to avoid potential interference between systems.

✓ A narrowband scheme typically makes use of the cell configuration illustrated in Figure 13.2.

✓ Adjacent cells use non-overlapping frequency bands within the overall 18-GHz band.

✓ It can assure that independent LANs in nearby geographical locations do not interfere with one another.

- ✓ To provide security from eavesdropping, all transmissions are encrypted

ADVANTAGE

- ❖ It guarantees interference-free communication.
- ❖ Unlike unlicensed spectrum, such as ISM, licensed spectrum gives the license holder a legal right to an interference-free data communications channel.
- ❖ Users of an ISM-band LAN are at risk of interference disrupting their communications, for which they may not have a legal remedy.

➔ **Unlicensed Narrowband RF**

- ✓ In 1995, RadioLAN became the first vendor to introduce a narrowband wireless LAN using the unlicensed ISM spectrum.
- ✓ This spectrum can be used for narrowband transmission at low power (0.5 watts or less).
- ✓ The RadioLAN product operates at 10 Mbps in the 5.8-GHz band.
- ✓ The product has a range of 50 m in a semiopen office and 100 m in an open office.
- ✓ The RadioLAN product makes use of a peer-to-peer configuration with an interesting feature.
- ✓ As a substitute for a stationary hub, the RadioLAN product automatically elects one node as the Dynamic Master, based on parameters such as location, interference, and signal strength.
- ✓ The identity of the master can change automatically as conditions change.
- ✓ The LAN also includes a dynamic relay function, which allows each station to act as a repeater to move data between stations that are out of range of each other.

3.2 To Understand Wi-Fi and IEEE 802.11 standard

3.2.1 Describe IEEE 802 Architecture

- ❖ The architecture of a LAN is best described in terms of a layering of protocols that organize the basic functions of a LAN.

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, 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 14.1 relates the LAN protocols to the OSI architecture. 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. 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
    - o Encoding/decoding of signals (e.g., PSK, QAM, etc.)
    - o Preamble generation/removal (for synchronization)
    - o Bit transmission/reception
- ❖ The physical layer of the 802 model includes a specification of the transmission medium and the topology. This is considered "below" the lowest layer of the OSI model. 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:

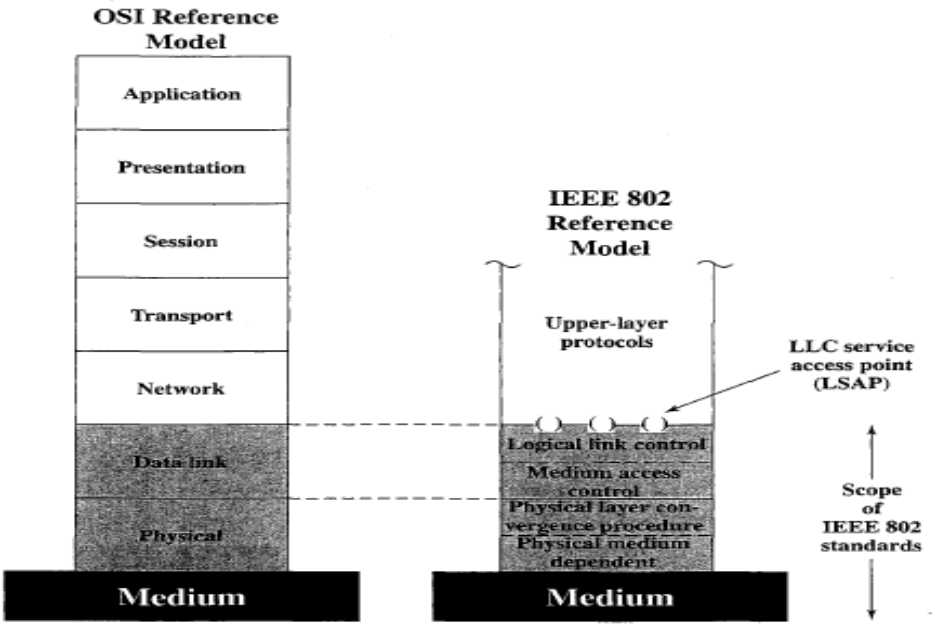


Figure 14.1 IEEE 802 Protocol Layers Compared to OSI Model

TWO SUBLAYERS:-

1. **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
2. **Physical medium dependent sublayer (PMD):** 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.

SERVICES:-

• 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).**

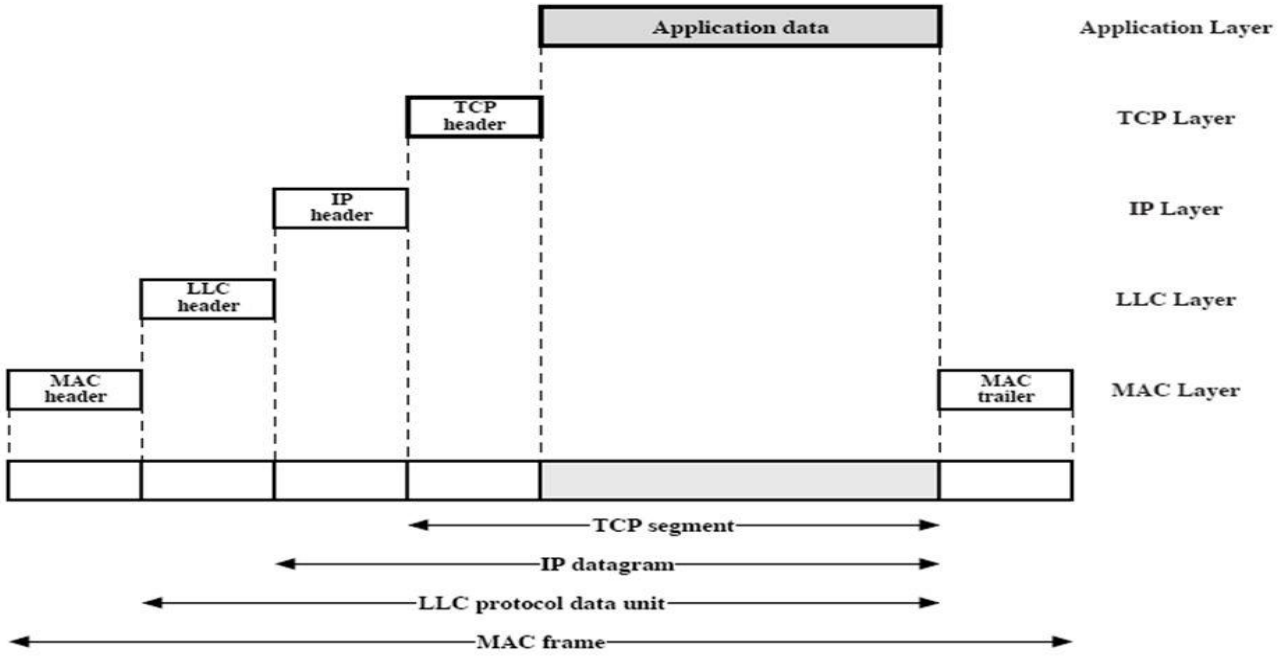


Figure 11.15 IEEE 802.16 Protocols in Context

- Figure 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 ofTCP/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.

FRAME FORMAT

- 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 14.3.
- The fields of this frame are as follows:

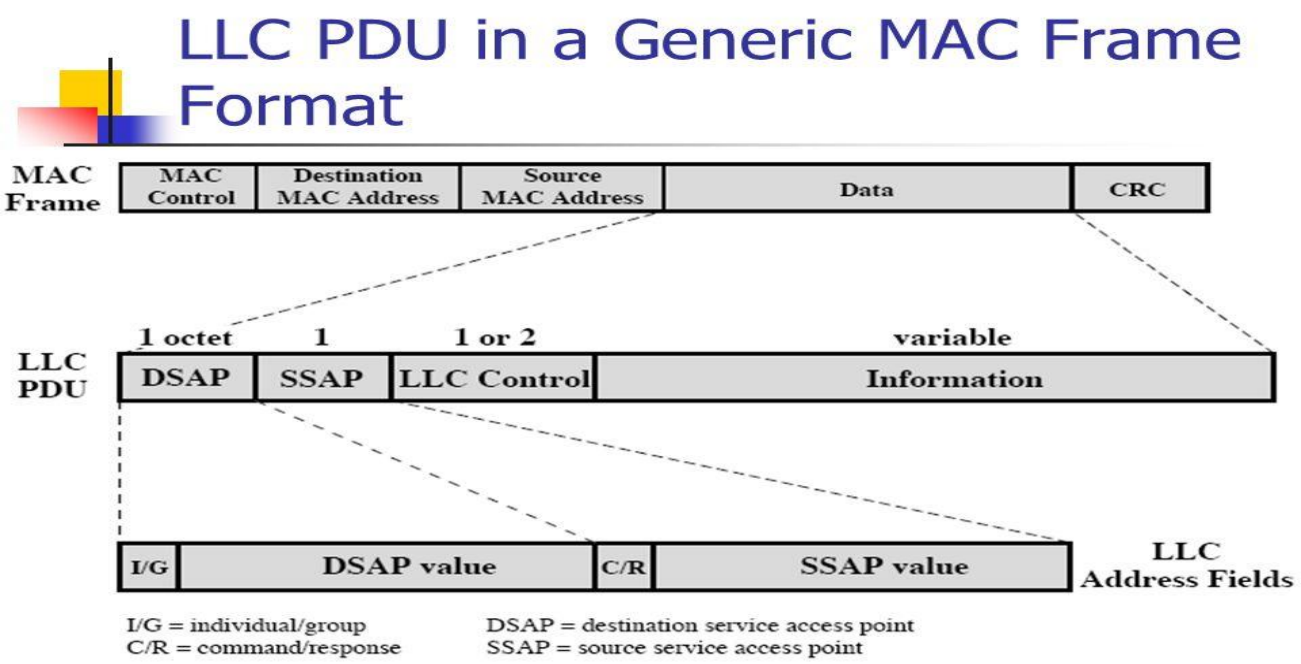


Figure 14.3 LLC PDU in a Generic MAC Frame Format

• **MAC Control:** 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, PCS, field). This is an error-detecting code, as described in Section 8.1. The CRC is used in virtually all data link protocols, such as HDLC.

…….

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 multi-access, shared-medium nature of the link (this differs from a multi-drop 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.
- ❖ 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:

1. **Unacknowledged connectionless service:** This is a datagram-style service. It is a very simpleservice 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.
2. **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.
3. **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.

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).

3.2.2 Explain IEEE 802.11 Architecture and services

Table 14.2 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

- ❖ In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, specifically devoted to wireless LANs, with a charter to develop a MAC protocol and physical medium specification.
- ❖ The initial interest was in developing a wireless LAN operating in the ISM (industrial, scientific, and medical) band.
- ❖ Since that time, the demand for WLANs, at different frequencies and data rates, has exploded.

IEEE 802.11 Architecture

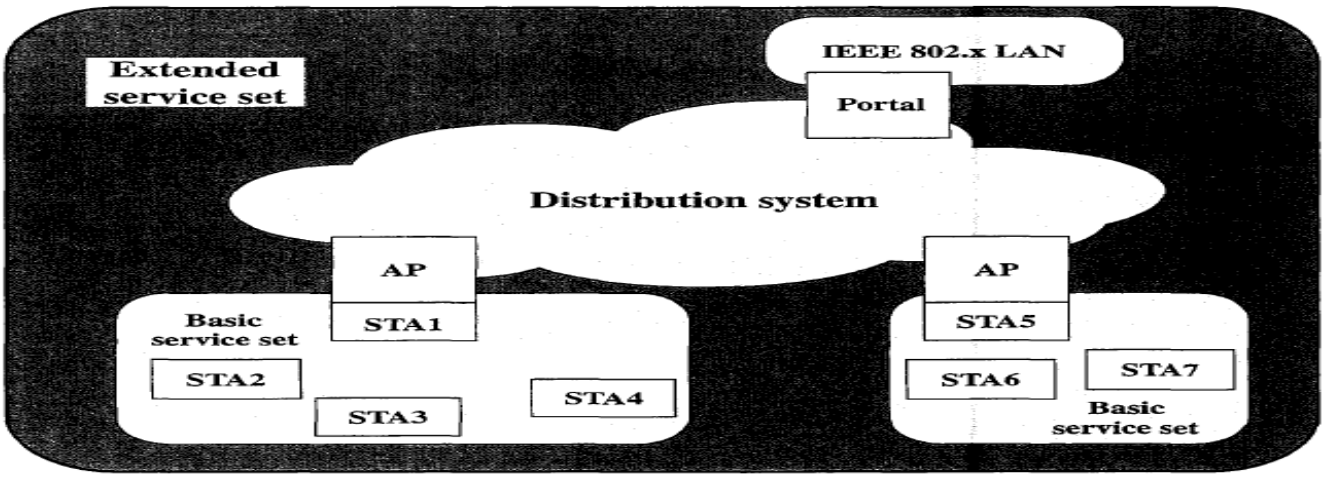


Figure 14.4 IEEE 802.11 Architecture

- Figure 14.4 illustrates the model developed by the 802.11 working group.

BSS

- The smallest building block of a wireless LAN 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 14.4, 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.

ESS An **extended service set (ESS)** consists of two or more basic service sets interconnected by a distribution system.

- Typically, the distribution system is a wired backbone LAN but can be any communications network. The extended service set appears as a single logical LAN to the logical link control (LLC) level.

- Figure 14.4 indicates that an access point (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 14.3 lists services and indicates two ways of categorizing them.

Table 14.3 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

1. The service provider can be either the station or the distribution system (DS). Station services are implemented in every 802.11 station, including access point (AP) stations. Distribution services are provided between basic service sets (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 a LLC PDU 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.

I) MSDU delivery is the basic service.

II) 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 14.4.
- 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.

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.

III) 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:

1. **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.
2. **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.
3. **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. To meet this requirement, a station must maintain an association with the AP within its current BSS. Three services relate to this requirement:

1. **Association:** Establishes an initial association between a station and an AP Before a station can transmit or receive frames on a wireless LAN, 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.
2. **Reassociation:** Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
3. **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.

IV) Access and Privacy Services

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 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 must also be attached to the wired LAN. On the other hand, with a wireless LAN, any station within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

IEEE 802.11 defines three services that provide a wireless LAN with these two features:

1. **Authentication:** Used to establish the identity of stations to each other. In a wired LAN, it is generally assumed that access to a physical connection conveys authority to connect to the LAN. This is not a valid assumption for a wireless LAN, in which connectivity is achieved simply by having an attached antenna that

is properly tuned. The authentication service is used by stations to establish their identity with stations they wish to communicate with. IEEE 802.11 supports several authentication schemes and allows for expansion of the functionality of these schemes. The standard does not mandate any particular authentication scheme, which could range from relatively unsecure handshaking to public key encryption schemes. However, IEEE 802.11 requires mutually acceptable, successful authentication before a station can establish an association with an AP.

2. **De-authentication:** This service is invoked whenever an existing authentication is to be terminated.
3. **Privacy:** Used to prevent the contents of messages from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

3.2.3 Explain IEEE 802.11 Medium Access Control

IEEE 802.11 MAC layer covers **three** functional areas: **reliable data delivery, medium access control**, and **security**.

Reliable Data Delivery: A wireless LAN using 802.11 physical and MAC layers is subject to considerable unreliability. Noise, interference, and other propagation effects result in 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. Timers used for retransmission at higher layers are on order of seconds. It is more efficient to deal with errors at MAC level. For this, 802.11 includes a frame exchange protocol.

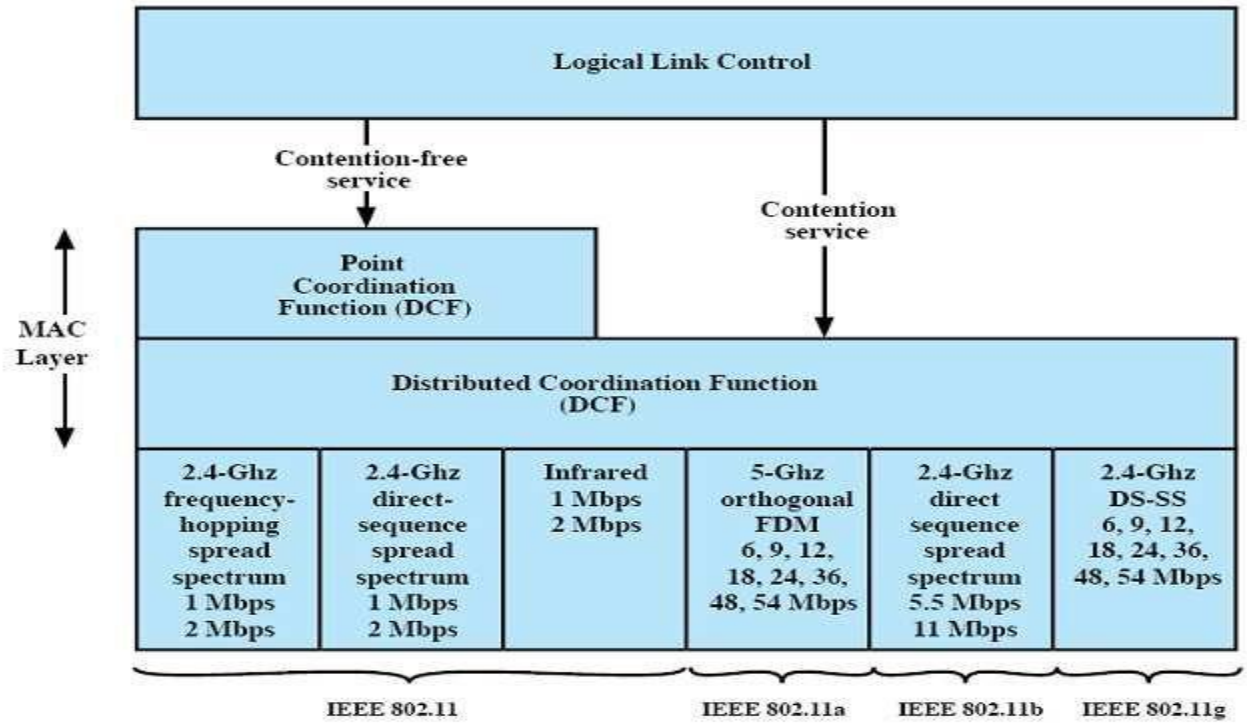
When a station receives a data frame from another station, it returns an acknowledgment (ACK) frame to source station. This exchange is treated as an atomic unit, not to be interrupted by a transmission from any other station. If source does not receive an ACK within a short period of time, either because its data frame was damaged or because returning ACK was damaged, source retransmits frame.

Basic data transfer mechanism in 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 destination. Destination then responds with a clear to send (CTS).After receiving CTS, source transmits data frame, and destination responds with an ACK. RTS alerts all stations that are within reception range of source that an exchange is under way; these stations refrain from transmission in order to avoid a collision between two frames transmitted at same time. Similarly, CTS alerts all stations that are within reception range of destination that an exchange is under way. RTS/CTS portion of exchange is a required function of MAC but may be disabled.

Medium Access Control: 802.11 group consider two types of MAC: **distributed access protocols**, which, like Ethernet, distribute decision to transmit over all 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 wireless LAN 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 is 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 14.5 illustrates architecture. The lower sublayer of MAC layer is **distributed coordination function (DCF)**. DCF uses a contention algorithm to provide access to all traffic. Ordinary asynchronous traffic directly uses DCF.

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.



DCF sub layer makes use of a simple CSMA (carrier sense multiple access) algorithm, which functions as follows. If a station has a MAC frame to transmit, it listens to medium. If medium is idle, station may transmit; otherwise station must wait until current transmission is complete before transmitting. 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 signals on medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and effects of its own transmission. To ensure smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme.

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

3.2.4. IEEE 802.11 Physical Layer

Physical layer for 802.11 has been issued in four stages. The first part, simply called IEEE 802.11, includes MAC layer and three physical layer specifications, two in 2.4-GHz band (ISM) and one in infrared, all operating at 1 and 2 Mbps. IEEE 802.11a operates in 5-GHz band at data rates up to 54 Mbps. IEEE 802.11b operates in 2.4-GHz band at 5.5 and 11 Mbps. IEEE 802.11g also operates in 2.4-GHz band, at data rates up to 54 Mbps.

Original IEEE 802.11 Physical Layer: Three physical media are defined in original 802.11 standard:

- Direct sequence spread spectrum (DSSS) operating in 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps.
- Frequency-hopping spread spectrum (FHSS) operating in 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps.
- Infrared at 1 Mbps and 2 Mbps operating at a wavelength between 850 and 950nm

3.2.5 Wi·Fi Protected Access

The original 802.11 specification included a set of security features for privacy and authentication which, unfortunately, were quite weak. For **privacy** 802.11 defined Wired Equivalent Privacy (WEP) algorithm. WEP makes use of RC4 encryption algorithm using a 40-bit key. A later revision enables use of a 104-bit key. For **authentication,** 802.11 requires that two parties share a secret key not shared by any other party and defines a protocol by which this key can be used for mutual authentication.

The privacy portion of 802.11 standard contained major weaknesses. 40-bit key is woefully inadequate. Even 104-bit key proved to be vulnerable, due to a variety of weaknesses both internal and external to protocol supporting WEP. These vulnerabilities include heavy reuse of keys, ease of data access in a wireless network, and lack of any key management within protocol. Similarly, there are a number of problems with shared-key authentication scheme.

802.11i task group has developed a set of capabilities to address WLAN security issues. To accelerate introduction of *strong* security into WLANs, 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 current state of 802.11i standard. As 802.11i evolves, WPA will evolve to maintain compatibility.

IEEE 802.11i addresses three main security areas: authentication, key management, and data transfer privacy. To improve authentication, 802.11i requires use of an authentication server (AS) and defines a more robust authentication protocol.

AS also plays a role in key distribution. For privacy, 802.11i provides three different encryption schemes. The scheme that provides a long-term solution makes use of Advanced Encryption Standard (AES) with 128-bit keys. Because the use of AES requires expensive upgrades to existing equipment, alternatives based on 104-bit RC4 are also defined.

Figure 14.13 gives a general overview of 802.11i operation. First, an exchange between a station and an AP enables two to agree on a set of security capabilities to be used. Then an exchange involving AS and station pro vides for secure authentication. AS is responsible for key distribution to AP, which in turn, manages and distributes keys to stations. Finally, strong encryption is used to protect data transfer between station and AP.

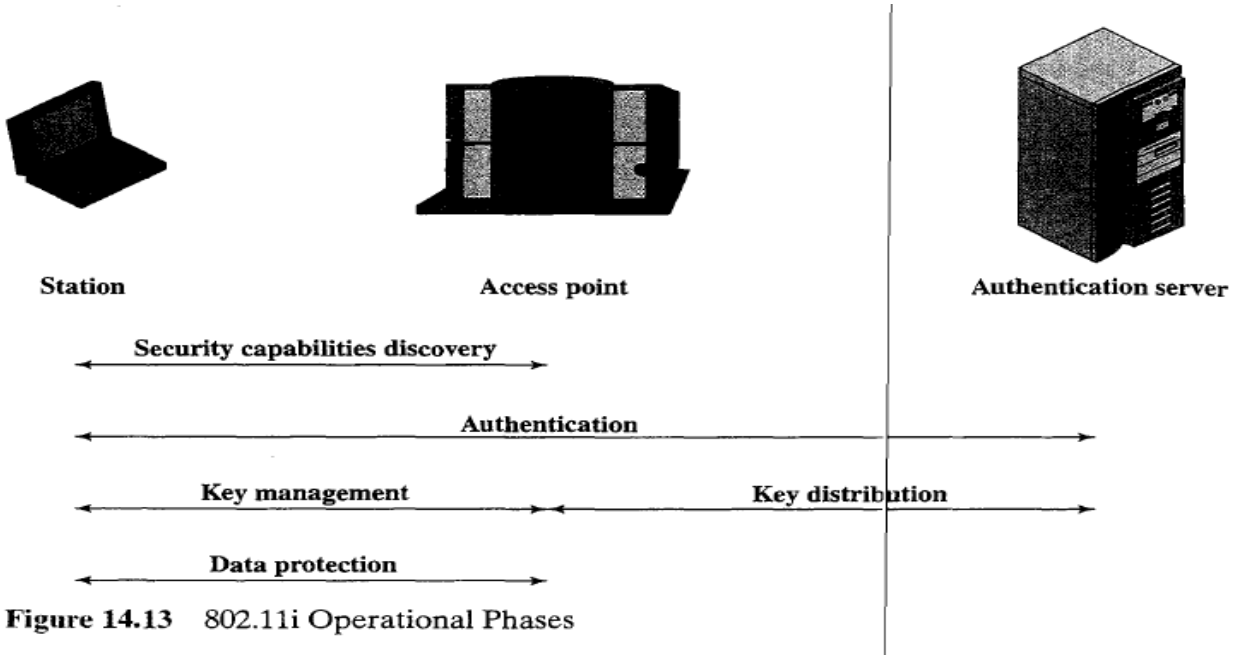


Figure 14.13 802.11i Operational Phases

802.11i architecture consists of three main ingredients:

• **Authentication:** A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between client and AP over wireless link.

• **Access control:** This function enforces use of authentication function, routes 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 data have not been altered.

Authentication operates at a level above LLC an MAC protocols and is considered beyond the scope of 802.11. There are a number of popular authentication protocols in use, including Extensible Authentication Protocol (EAP) and Remote Authentication Dial-In User Service (RADIUS).