LOCAL AREA NETWORKS

The development of LANs was motivated by the need to share resources and information among workstations in a department or workgroup. The short distances between computers imply that low-cost, high-speed, reliable communications is possible.

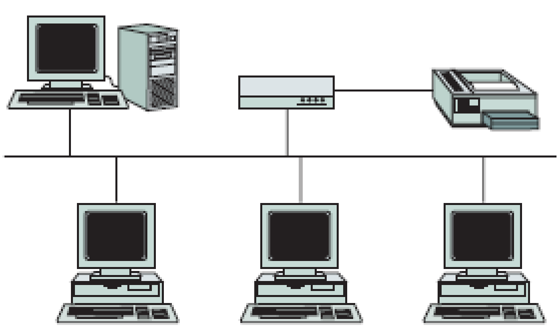
In this section we discuss general aspects of LAN standards. Most LAN standards have been developed by the IEEE 802 committee of the Institute of Electrical and Electronic Engineers (IEEE), which has been accredited in the area of LANs by the American National Standards Institute (ANSI).

LAN Structure

The structure of a typical LAN is shown in Figure below. A number of computers and network devices such as printers are interconnected by a shared transmission medium, typically a cabling system, which is arranged in a bus, ring, or star topology. The cabling system may use twisted-pair cable, coaxial cable, or optical fiber transmission media. In some cases the cabling system is replaced by wireless transmission based on radio or infrared signals.

LAN standards define physical layer protocols that specify the physical properties of the cabling or wireless system, for example, connectors and maximum cable lengths, as well as the digital transmission system, for example, modulation, line code, and transmission speed.

The computers and network devices are connected to the cabling system through a network interface card (NIC). The NIC card coordinates the transfer of information between the computer and the network. The NIC card transfers information in parallel format to and from main memory (RAM) in the computer.



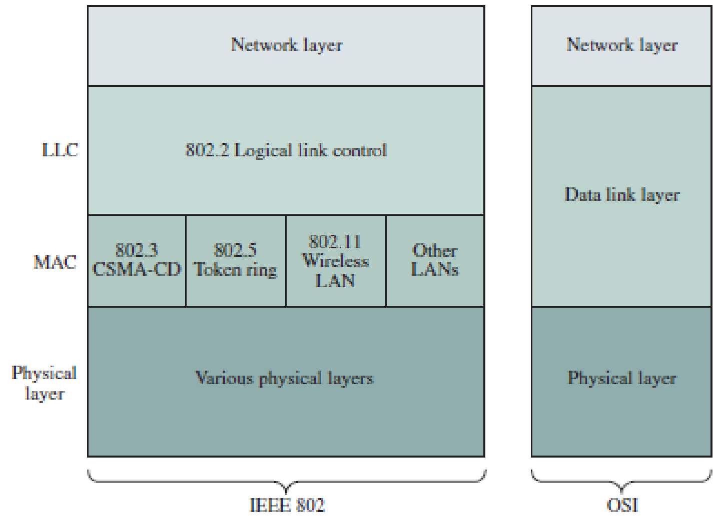
Typical LAN structure

The NIC card includes read-only memory (ROM) containing firmware that allows the NIC to implement the MAC protocol of a LAN standard. This process involves taking network layer PDUs, encapsulating them inside MAC frames, and transferring the frames by using the MAC algorithm, as well as receiving MAC frames and delivering the network layer PDUs to the computer.

The Medium Access Control Sublayer

The layered model in below Figure shows how the LAN functions are placed within the two lower layers of the OSI reference model. The data link layer is divided into two sublayers the logical link control (LLC) sublayer and the medium access control (MAC) sublayer.

The MAC sublayer deals with the problem of coordinating the access to the shared physical medium. The MAC layer provides the connectionless transfer of datagrams. The MAC entity accepts a block of data from the LLC sublayer or directly from the network layer. This entity constructs a PDU that includes source and destination MAC addresses as well as a frame check sequence (FCS), which is simply a CRC checksum. The main task of the MAC entities is to execute the MAC protocol that directs when they should transmit the frames into the shared medium.



IEEE 802 LAN standards

The Logical Link Control Layer

The IEEE 802 committee has also defined a logical link control (LLC) sublayer that operates over all MAC standards. The LLC provides a means for exchanging frames between LANs that use different MAC protocols.

The LLC builds on the MAC datagram service to provide three services:

- Type 1 LLC service is unacknowledged connectionless service that uses unnumbered frames to transfer unsequenced information. Type 1 LLC service is by far the most common in LANs.
- Type 2 LLC service uses information frames and provides reliable connection-oriented service. A connection setup and release is required, and the connection provides for error control, sequencing, and flow control. Type 2 operation is useful when the end systems do not use a transport layer protocol to provide reliable service.
- Type 3 LLC service provides acknowledged connectionless service, that is, connectionless transfer of individual frames with acknowledgments.

LAN STANDARDS

In this section we discuss the structure of the important LAN standards.

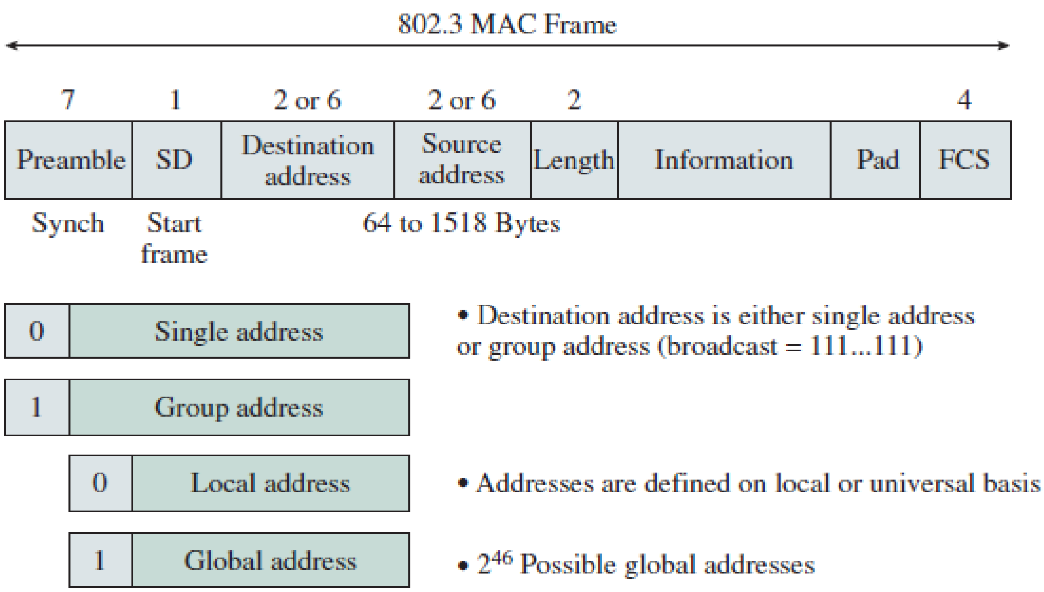
Ethernet and IEEE 802.3 LAN Standard

The original 802.3 standard was defined for a bus-based coaxial cable LAN in which terminal transmissions are broadcast over the bus medium using Carrier Sensing Multiple Access with Collision Detection (CSMA-CD) for the MAC protocol. A station with a frame to transmit waits until the channel is silent. When the channel goes silent, the station transmits but continues to listen for collisions that can occur if other stations also begin to transmit. If a collision occurs, the station aborts the transmission and schedules a later random time when it will reattempt to transmit its frame. If a collision does not occur within two propagation delay times, then the station knows that it has captured the channel, as the station’s transmission will have reached all stations and so they will refrain from transmitting until the first station is done. A minislot time defines a time duration that is at least as big as two propagation delays.

The critical parameter in the CSMA-CD system is the minislot time that forms the basis for the contention resolution that is required for a station to seize control of the channel. The original 802.3 was designed to operate at 10 Mbps over a maximum distance of 2500 meters.

The IEEE 802.3 standard specifies that the rescheduling of retransmission attempts after a collision uses a truncated binary exponential back-off algorithm. If a frame is about to undergo its nth retransmission attempt, then its retransmission time is determined by selecting an integer in the range between 0 and 2^k-1, where k = min (n, 10) . That is, the first retransmission time involves zero or one minislot times; the second retransmission time involves 0, 1, 2, or 3 minislot times; and each additional slot retransmission extends the range by a factor of 2 until the maximum range of 210. The increased retransmission range after each collision is intended to increase the likelihood that retransmissions will succeed. Up to 16 retransmissions will be attempted, after which the system gives up.

Frame Structure



IEEE 802.3 MAC frame

Figure shows the MAC frame structure for the IEEE 802.3. The frame begins with a seven-octet preamble that repeats the octet 10101010. This pattern produces a square wave that allows the receivers to synchronize to the beginning of the frame. The preamble is followed by the start frame delimiter that consists of the pattern 10101011. The two consecutive 1s in the delimiter indicate the start of the frame.

The destination and source address fields follow. The address fields are six bytes long. (Two-byte address fields have been defined but are not used). The first bit of the destination address distinguishes between single addresses and group addresses that are used to multicast a frame to a group of users. The next bit indicates whether the address is a local address or a global address. Thus in the case of six-byte addresses, the standard provides for 246 global addresses. The first three bytes specify the NIC vendor, so this scheme allows up to 224 16,777,215 addresses per vendor.

There are three types of physical addresses. Unicast addresses are the unique address permanently assigned to a NIC card. The card normally matches transmissions against this address to identify frames destined to it. Multicast addresses identify a group of stations that are to receive a given frame. NIC cards are set by their host computer to accept specific multicast addresses. Multicasting is an efficient way of distributing information in situations where multiple entities or processes require a piece of information as, for example, in the spanning tree algorithm. The broadcast address, indicated by the all 1s physical address, indicates that all stations are to receive a given packet.

The length field indicates the number of bytes in the information field. The longest allowable 802.3 frame is 1518 bytes, including the 18-byte overhead but excluding the preamble and SD. The pad field ensures that the frame size is always at least 64 bytes long.

The last field is the CCITT 32-bit CRC check. The CRC field covers the address, length information, and pad fields. Upon receiving a frame, the NIC card checks to see that the frame is of an acceptable length and then checks the received CRC for errors. If errors are detected, the frame is discarded and not passed to the network layer.

FAST ETHERNET

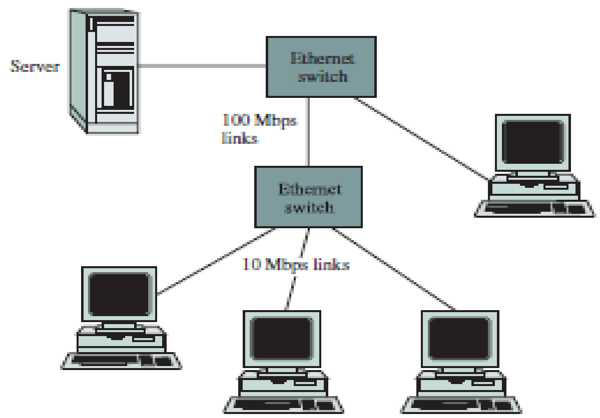
The IEEE 802.3u standard was approved in 1995 to provide Ethernet LANs operating at 100 Mbps. We refer to systems that operate under this standard as Fast Ethernet. To maintain compatibility with existing standards, the frame format, interfaces, and procedures have been kept the same. The performance of the CSMA-CD medium access control is sensitive to the ratio of the round-trip propagation delay and the frame transmission time. To obtain good performance, this ratio must be small. When the transmission speed is increased from 10 Mbps to 100 Mbps, the packet transmission time is reduced by a factor of 10. For the MAC protocol to operate correctly, either the size of the minimum frame must be increased by a factor of 10 to 640 bytes or the maximum length between stations is reduced by a factor of 10 to, say, 250 meters.

The decision in developing the 100 Mbps IEEE 802.3u standard was to keep frame sizes and procedures unchanged and to define a set of physical layers that were entirely based on a hub topology involving twisted pair and optical fiber. Coaxial cable was not included in the standard. The standard involves stations that use unshielded twisted-pair (UTP) wiring to connect to hubs in a star topology.

To obtain a bit rate of 100 Mbps, the 100BaseT4 standard uses four UTP 3 wires. The 100 Mbps transmission is divided among three of the twisted pairs and flows in one direction at a time. The 100BaseTX uses two UTP 5 wires. One pair of wires is for transmission and one for reception, so 100BaseTX can operate in full-duplex mode. A 100BaseFX standard has also been provided that uses two strands of multimode optical to provide full-duplex transmission at 100 Mbps in each direction. The 100BaseFX system can reach over longer distances than the twisted pair options.

The 100 Mbps IEEE 802.3 standards provide for two modes of operations at the hubs. In the first mode all incoming lines are logically connected into a single collision domain, and the CSMA-CD MAC procedure is applied. In the second approach the CSMA-CD procedure is not used, and instead the IEEE 802.3 standard simply provides a means of accessing based on multiplexing and switching.

Fast Ethernet LANs can be used to provide higher bandwidth in campus backbones and in the access portions of the network where packet flows are aggregated. The scenario in which Fast Ethernet hubs are used to (1) aggregate traffic from shared 10 Mbps LANs, (2) provide greater bandwidth to a server, and (3) provide greater bandwidth to individual users.



Application of Fast Ethernet

GIGABIT ETHERNET

The IEEE 802.3z Gigabit Ethernet standard was completed in 1998 and established an Ethernet LAN that increased the transmission speed over that of Fast Ethernet by a factor of 10. The goal was to define new physical layers but to again retain the frame structure and procedures of the 10 Mbps IEEE 802.3 standard.

The increase in speed by another factor of 10 put a focus on the limitations of the CSMA-CD MAC algorithm. For example, at a 1 Gbps speed, the transmission of a minimum size frame of 64 bytes can result in the transmission being completed before the sending station senses a collision. For this reason, the slot time was extended to 512 bytes. Frames smaller than 512 bytes must be extended with an additional carrier signal, in effect resulting in the same overhead as in padding the frame. In addition, an approach called packet bursting was introduced to address this scaling problem. Stations are allowed to transmit a burst of small packets, in effect to improve the key ratio a. Nevertheless, it is clear that with Gigabit Ethernet the CSMA-CD access control reached the limits of efficient operation. In fact, the standard preserves the Ethernet frame structure but operates primarily in a switched mode.

Gigabit Ethernet physical layer standards have been defined for multimode fiber with maximum length of 550 m, single-mode fiber with maximum length of 5 km, and four-pair category 5 UTP at a maximum length of up to 100 m.

Wireless LANs and IEEE 802.11 Standard

Wireless technology, in the form of digital radio and infrared transmission, can eliminate many of the wires and, in the process, simplify the installation and movement of equipment, as well as provide connectivity between computers. Wireless technology, however, must overcome significant challenges:

• Radio and infrared transmission is susceptible to noise and interference, so such transmission is not very reliable.
• The strength of a radio transmission varies in time and in space and so coverage is inconsistent and unpredictable.
• The transmitted signal cannot easily be contained to a specific area, so signals can be intercepted by eavesdroppers.
• The spectrum is finite and must be shared with other users (your neighbor's wireless LAN), and devices (e.g., microwave ovens and florescent lamps!).
• The limited spectrum also makes it difficult to provide the high transmission speeds that are easily

attained using wired media.

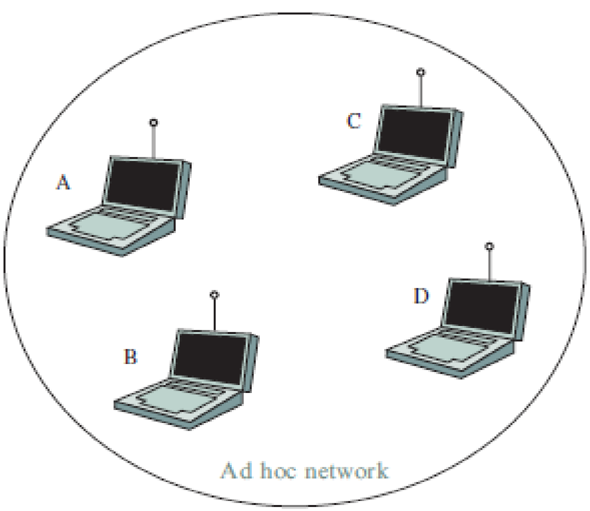
• Radio spectrum has traditionally been regulated differently by different government administrations, so it can be difficult to design products for a global market.

The most compelling reason for wireless networks, however, is that they enable user mobility. In the context of wireless LANs, user mobility is particularly significant in situations where users carry portable computers or devices that need to communicate to a server or with each other. To provide mobility, further challenges must be overcome:

Mobile devices operate on batteries, so the MAC protocols must incorporate power management procedures. Protocols need to be developed that enable a station to discover neighbors in the local network and to provide seamless connections even as users roam from one coverage area to another.

In this section we focus on the IEEE 802.11 LAN standard that specifies a MAC layer that is designed to operate over a number of physical layers. In addition to the basic issue of coordinating access, the standard must incorporate error control to overcome the unreliability of the channel, modified addressing and association procedures to deal with station portability and mobility, and inter-connection procedures to extend the reach of a wireless stations.

AD HOC AND INFRASTRUCTURE NETWORKS



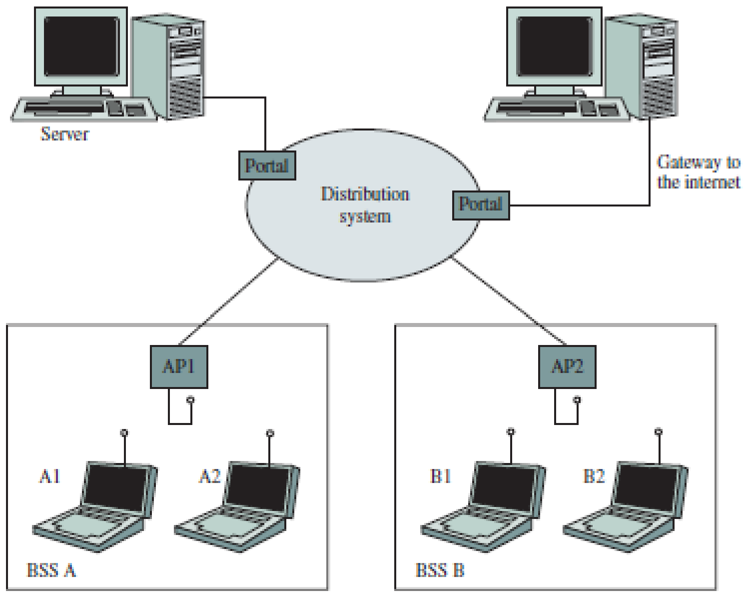
The basic service set (BSS) is the basic building block of the IEEE 802.11 architecture. A BSS is defined as a group of stations that coordinate their access to the medium under a given instance of the medium access control. The geographical area covered by the BSS is known as the basic service area (BSA). A BSA may extend over an area with a diameter of tens of meters. Conceptually, all stations in a BSS can communicate directly with all other stations in a BSS.

A single BSS can be used to form an ad hoc network. An ad hoc network consists of a group of stations within range of each other. Ad hoc networks are typically temporary in nature. They can be formed spontaneously anywhere and be disbanded after a limited period of time. Figure (left side) is an illustration of an ad hoc network.

In 802.11 a set of BSSs can be interconnected by a distribution system to form an extended service set (ESS) as shown in Figure below. Each BSS has an access point (AP) that has station functionality and provides access to the distribution system. The AP is analogous to the base station in a cellular communications network. An ESS can also provide gateway access for wireless users into a wired network such as the Internet. This access is accomplished via a device known as a portal. The term infrastructure network is used informally to refer to the combination of BSSs, a distribution system, and portals.

To join an infrastructure BSS, a station must select an AP and establish an association with it. This procedure establishes a mapping between the station and the AP that can be provided to the distribution system. The station can then send and receive data messages via the AP. A re-association service allows a station with an established association to move its association from one AP to another AP. The dissociation service is used to terminate an existing association. Stations have the option of using an authentication service to establish the identity of other stations. Stations also have the option of using a privacy service that prevents the contents of messages from being read by anyone other than the intended recipient(s).

In wired LANs the MAC address specifies the physical location of a station, since users are stationary. In wireless LANs, the MAC address identifies the station but not the location, since the standard assumes that stations can be portable or mobile. A station is portable if it can move from one location to another but remains fixed while in use. A mobile station moves while in use.



Infrastructure network and extended service set

FRAME STRUCTURE AND ADDRESSING

IEEE 802.11 supports three types of frame: management frames, control frames, and data frames. The management frames are used for station association and disassociation with the AP, timing and synchronization, and authentication and de-authentication. Control frames are used for handshaking and for positive acknowledgments during the data exchange. Data frames are used for the transmission of data. The MAC header provides information on frame control, duration, addressing, and sequence control. Figure above shows that the format of the MAC frame consists of a MAC header, a frame body, and a CRC checksum.

- The frame control field in the MAC header is 16 bits long, and it specifies the following items:

• The 802.11 protocol version (the current version is 0).

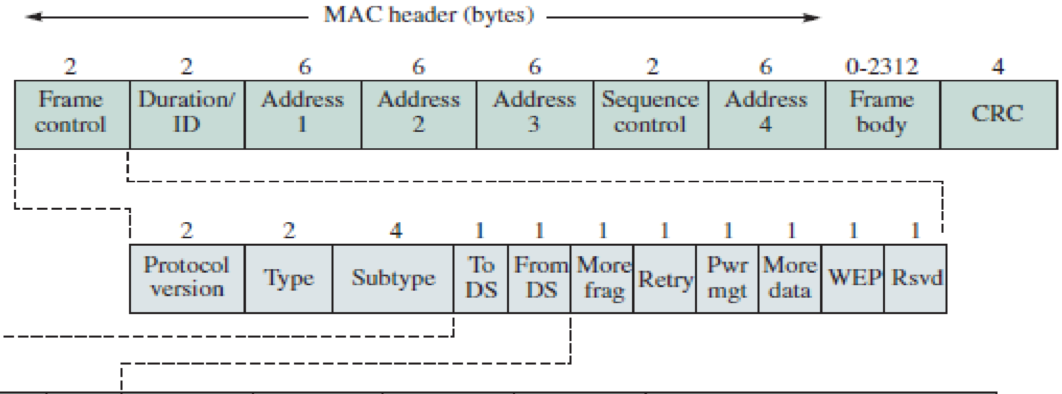
• The type of frame, that is, management (00), control (01), or data (10).

• The subtype within a frame type, for example, type = “management” Subtype = “association request” or type = “control” subtype = “ACK”

• The *To DS* field is set to 1 in Data type frames destined for the distribution system.

• The *From DS* field is set to 1 in Data type frames exiting the distribution system.

• The more fragments field is set to 1 in frames that have another fragment of the current MSDU to follow.



To DS	From DS	Address 1	Address 2	Address 3	Address 4	Meaning
0	0	Destination address	Source address	BSS ID	N/A	Data frame from station to station within a BSS
0	1	Destination address	BSS ID	Source address	N/A	Data frame exiting the DS
1	0	BSS ID	Source address	Destination address	N/A	Data frame destined for the DS
1	1	Receiver address	Transmitter address	Destination address	Source address	WDS frame being distributed from AP to AP

DS = distribution system AP = access point

IEEE 802.11 frame structure

- The retry field is set to 1 in Data or Management type frames that are retransmissions of an earlier frame.
- The power management bit is set to indicate the power management mode of a station.
- The more data field is set to 1 to indicate to a station in power save mode that more MSDUs are buffered for it at the AP.
- The Wired Equivalent Privacy (WEP) field is set to 1 if the frame body field contains information that has been processed by the cryptographic algorithm.

The durationID field in the MAC header is 16 bits long and usually contains a duration value (net allocation vector) that is used in the MAC algorithm.

Addresses are 48-bit long IEEE 802 MAC addresses and can be individual or group (multicast/broadcast). The BSS identifier (BSS ID) is a 48-bit field of the same format as IEEE 802 MAC addresses, uniquely identifies a BSS. The destination address is an IEEE MAC individual or group address that specifies the MAC entity that is the final recipient of the MSDU that is contained in the frame body field. The source address is a MAC individual address that identifies the MAC entity from which the MSDU originated. The receiver address is a MAC address that identifies the intended immediate recipient station for the MPDU in the frame body field. The transmitter address is a MAC individual address that identifies the station that transmitted the MPDU contained in the frame body field.

To DS = 0, From DS = 0: This case corresponds to the transfer of a frame from one station in the BSS to another station in the same BSS.

To DS = 0, From DS = 1: This case corresponds to the transfer of a frame from the distribution system to a station in the BSS.

To DS = 1, From DS = 0: This case corresponds to the transfer of a frame from a station in the BSS to the distribution system.

To DS = 1, From DS 1: This special case applies when we have a wireless distribution system (WDS) transferring frames between BSSs.

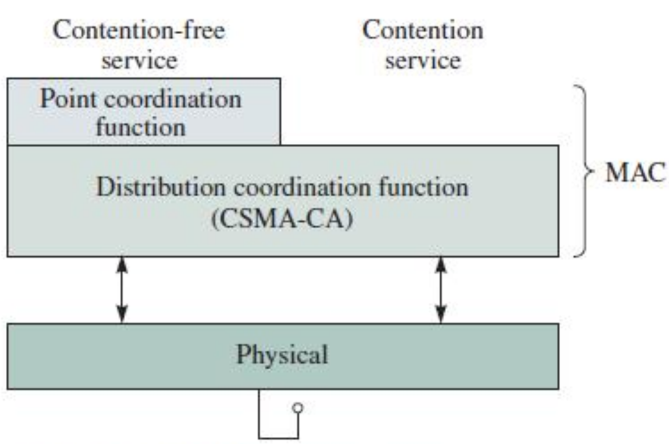
The sequence control field is 16 bits long, and it provides 4 bits to indicate the number of each fragment of an MSDU and 12 bits of sequence numbering for a sequence number space of 4096. The frame body field contains information of the type and subtype specified in the frame control field. For Data type frames, the frame body field contains an MSDU or a fragment of an MSDU. Finally, the CRC field contains the 32-bit cyclic redundancy check calculated over the MAC header and frame body field.

Medium Access Control

The MAC sublayer is responsible for the channel access procedures, protocol data unit (PDU) addressing, frame formatting, error checking, and fragmentation and reassembly of MSDUs (MAC Service Data Unit). The MAC layer also provides options to support security services through authentication and privacy mechanisms.

The IEEE 802.11 MAC protocol is specified in terms of coordination functions that determine when a station in a BSS is allowed to transmit and when it may be able to receive PDUs over the wireless medium. The distributed coordination function (DCF) provides support for asynchronous data transfer of MSDUs on a best-effort basis.

IEEE 802.11 also defines an optional point coordination function (PCF), which may be implemented by an AP, to support connection-oriented time-bounded transfer of MSDUs.

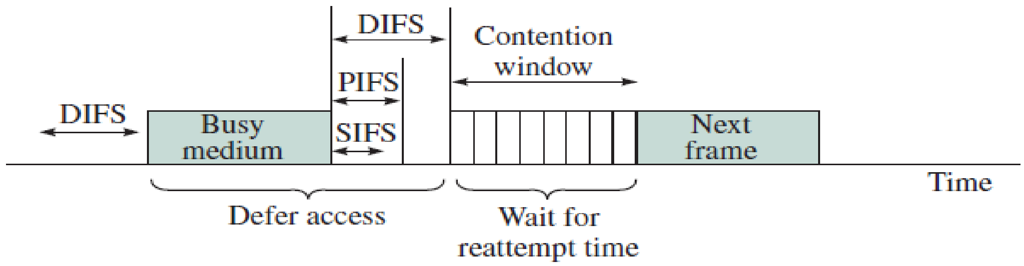


IEEE 802.11 MAC architecture

Distributed coordination function

The DCF is the basic access method used to support asynchronous data transfer on a best-effort basis. All stations are required to support the DCF. The access control in ad hoc networks uses only the DCF. Infrastructure networks can operate using just the DCF or a coexistence of the DCF and PCF.

The DCF is based on the carrier sensing multiple assess with collision avoidance (CSMA-CA) protocol. Carrier sensing involves monitoring the channel to determine whether the medium is idle or busy. If the medium is busy, the station should wait until the channel becomes idle. When this happens, the other stations may have also been waiting for the channel to become idle. If the algorithm is to transmit immediately after the channel becomes idle, then collisions are likely to occur; and because collision detection is not possible, the channel will be wasted for an entire frame duration. A solution to this problem is to randomize the times at which the contending stations attempt to seize the channel. This approach reduces the likelihood of simultaneous attempts.



Basic CSMA-CA operation

Figure shows the basic CSMA-CA operation. All stations are obliged to remain quiet for a certain minimum period after a transmission has been completed, called the interframe space (IFS). The length of the IFS depends on the type of frame that the station is about to transmit. High-priority frames must only wait the short IFS (SIFS) period before they contend for the channel. Frame types that use SIFS include ACK frames, CTS frames, data frames of a segmented MSDU and any frame from an AP during the CFP. The PCF interframe space (PIFS) is intermediate in duration and is used by the PCF to gain priority access to the medium at the start of a CFP. The DCF interframe space (DIFS) is used by the DCF to transmit data and management MPDUs.

A station is allowed to transmit an initial MAC PDU under the DCF method if the station detects the medium idle for a period DIFS or greater. However, if the station detects the medium busy, then it must calculate a random backoff time to schedule a reattempt. A station that has scheduled a reattempt monitors the medium and decrements a counter each time an idle contention slot occurs. The station is allowed to transmit when its backoff timer expires during the contention period. If another station transmits during the contention period before the given station, then the backoff procedure is suspended and resumed the next time a contention period takes place. When a station has successfully completed a frame transmission and has another frame to transmit, the station must first execute the backoff procedure. Stations that had already been contending for the channel tend to have smaller remaining backoff times when their timers are resumed, so they tend to access the medium sooner than stations with new frames to transmit. This behavior introduces a degree of fairness in accessing the channel.

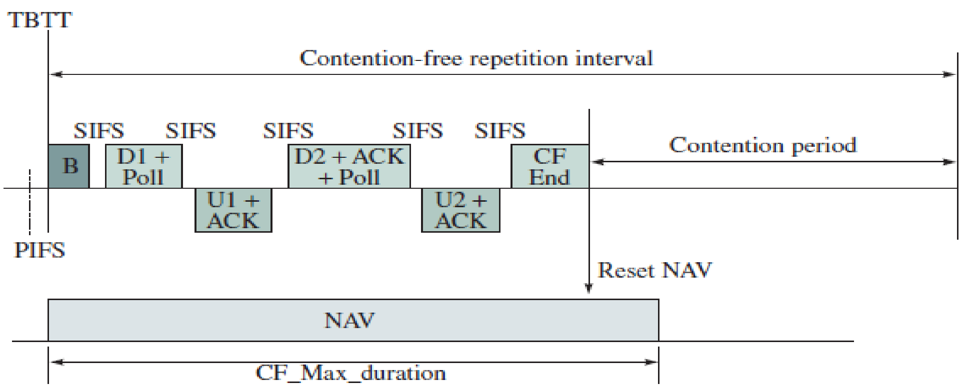
Point coordination function

The PCF is an optional capability that can be used to provide connection oriented, contention-free services by enabling polled stations to transmit without contending for the channel. The PCF function is performed by the **point coordinator** (PC) in the AP within a BSS. Stations within the BSS that are capable of operating in the CFP (contention free period) are known as **CF-aware stations**.

[*The term CFP defines a **period** of time during which access to the Wireless Medium is **free** of **contention**.*]

The PCF is required to coexist with the DCF and logically sits on top of the DCF. The CFP repetition interval (CFP_Rate) determines the frequency with which the PCF occurs. Within a repetition interval, a portion of the time is allotted to contention-free traffic, and the remainder is provided for contention-based traffic. The CFP repetition interval is initiated by a ***beacon frame*** **(***Beacon frame is one of the management **frames** which contains all* *the information about the network.* ***Beacon frames*** *are transmitted periodically to announce the presence of a wireless LAN.)*, where the beacon frame is transmitted by the AP. One of the AP's primary functions is synchronization and timing. Once the CFP_Rate is established, the duration of the CFP is determined. The maximum size of the CFP is determined by the manageable parameter, *CFP_Max_Duration*. At a minimum, time must be allotted for at least one MPDU to be transmitted during the CP (contention period). It is up to the AP to determine how long to operate the CFP during any given repetition interval. If traffic is very light, the AP may shorten the CFP and provide the remainder of the repetition interval for the DCF. The CFP may also be shortened if DCF traffic from the previous repetition interval carries over into the current interval.

Figure below is a sketch of the CFP repetition interval, illustrating the coexistence of the PCF and DCF. At the nominal beginning of each CFP repetition interval, the so-called target beacon transmission time (TBTT), all stations in the BSS update their NAV (*Network Allocation Vector- which indicates the amount of time that must elapse until the current transmission is complete*) to the maximum length of the CFP (i.e., *CFP_Max_Duration*). During the CFP, stations may transmit only to respond to a poll from the PC or to transmit an acknowledgment one SIFS interval after receipt of an MPDU. At the nominal start of the CFP, the PC senses the medium. If the medium remains idle for a PIFS interval, the PC transmits a beacon frame to initiate the CFP. In case the CFP is lightly loaded, the PC can foreshorten the CFP and provide the remaining bandwidth to contention-based traffic by issuing a CF-End or CF-End+Ack control frame. This action causes all stations that receive the frame in the BSS to reset their NAV values.

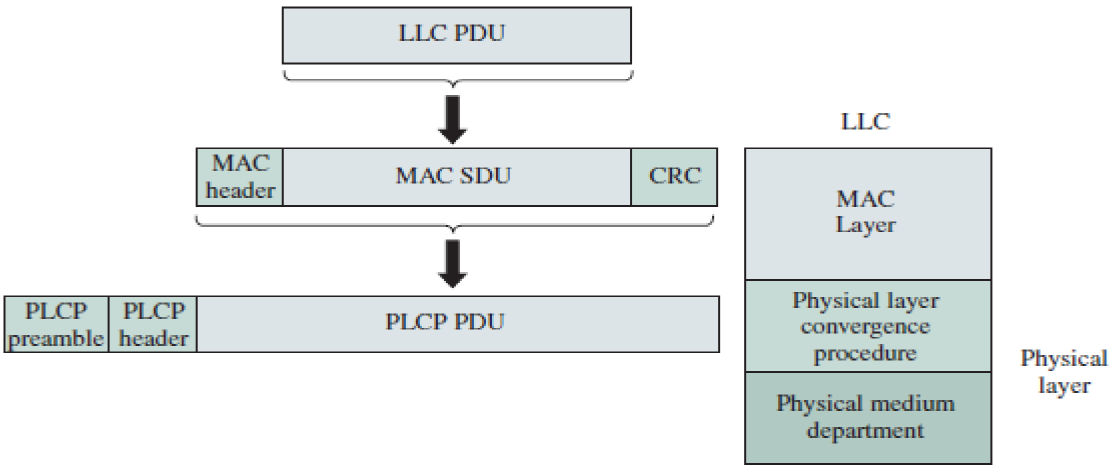


D1, D2 = frames sent by point coordinator
U1, U2 = frames sent by polled station
TBTT = target beacon transmission time
B = beacon frame

Point coordination frame transfer

PHYSICAL LAYERS

The IEEE 802.11 LAN has several physical layers defined to operate with its MAC layer. Each physical layer is divided into two sublayers that correspond to two protocol functions as shown in Figure. The physical layer convergence procedure (PLCP) is the upper sublayer, and it provides a convergence function that maps the MAC PDU into a format suitable for transmission and reception over a given physical medium. The physical medium dependent (PMD) sublayer is concerned with the characteristics and methods for transmitting over the wireless medium.



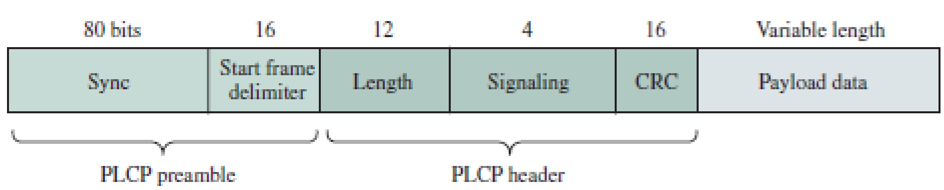
IEEE 802.11 physical layer

Figure shows that the MAC PDU is mapped into a PLCP frame that consists of three parts. The first part is a preamble that provides synchronization and start-of-frame information. The second part is a PLCP header that provides transmission bit rate and other initialization information as well as frame-length information and a CRC. The third part consists of the MAC PDU possibly modified (scrambled) to meet requirements of the transmission system. The specific structure of each PLCP depends on the particular physical layer definition. We next discuss **three physical layers** that have been defined for IEEE 802.11.

<u>Frequency hopping spread spectrum for the 2.4 GKHz ISM band</u>

Spread spectrum transmission is a form of digital modulation technique that takes a data signal of certain bit rate and modulates it onto a transmitted signal of much larger bandwidth. The spread spectrum receiver uses its knowledge of how the spreading was done to compress the received signal and recover the original data signal. Spread spectrum provides great robustness with respect to interference as well as other transmission impairments such as fading that results from multipath propagation. Frequency hopping is one type of spread spectrum technique.

Frequency hopping involves taking the data signal and modulating it so that the modulated signal occupies different frequency bands as the transmission progresses. To recover the signal, the receiver must know the sequence of channels that it should tune to as well as the “dwell” time in each channel.

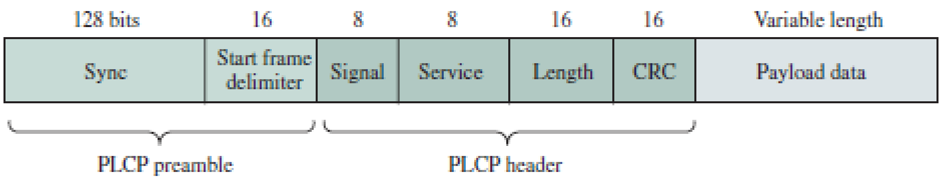


Frequency-hopping spread spectrum PLCP frame format

Figure shows the format of the PLCP frame. The PLCP preamble starts with 80 bits of 0101 synchronization pattern that the receiver uses to detect the presence of a signal and to acquire symbol timing. The preamble ends with a 16- bit start frame delimiter. The PLCP header consists of a 12-bit PLCP_PDU length indicator that allows for PLCP total lengths of up to 4095 bytes. The PLCP header also contains a four-bit field in which the first three bits are reserved and the last bit indicates operation at 1 Mbps or 2 Mbps. The last 16 bits of the PLCP header are a 16-bit CRC using the CCITT-16 generator polynomial that covers the preceding 16 bits in the header. The PLCP header is always transmitted at the base rate of 1 Mbps. The PLCP_PDU is formed by scrambling the binary sequence of the MAC PDU and converting it into the sequence of symbols that are suitable for the frequency shift keying modulation scheme that is used in the frequency hopping.

Direct sequence spread spectrum for the 2.4 GHz ISW band

Direct sequence spread spectrum (DSSS) is another method for taking a data signal of a given bit rate and modulating it into a signal that occupies a much larger bandwidth. DSSS represents each data 0 and 1 by the symbols -1 and +1 and then multiplies each symbol by a binary pattern of +1s and 1s to obtain a digital signal that varies more rapidly and occupies a larger frequency band. Each binary data bit results in the transmission of plus or minus the polarity of the Barker sequence. The Barker sequence provides good immunity against interference and noise as well as some protection against multipath propagation.



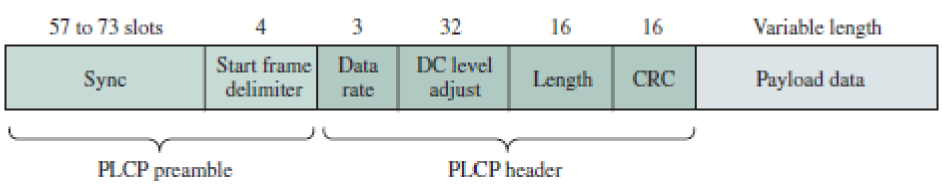
Direct sequence spread spectrum PLCP frame format

Figure shows the format of the PLCP frame. The PLCP preamble starts with 128 scrambled bits of synchronization that the receiver uses to detect the presence of a signal. The preamble ends with a 16-bit start frame delimiter that is used for bit synchronization. The PLCP header consists of an 8-bit signal field that indicates to the physical layer the modulation that is to be used for transmission and reception of the MPDU; an 8-bit service field that is reserved for future use; a 16-bit field that indicates the number of bytes in the MPDU, from 4 to 216; and a 16-bit CRC using the CCITT-16 generator polynomial. The PLCP header is always transmitted at the base rate of 1 Mbps.

Infrared physical layer

The IEEE 802.11 infrared physical layer operates in the near-visible light range of 850 to 950 nanometers. Diffuse transmission is used so the transmitter and receivers do not have to point to each other. The transmission distance is limited to the range 10 to 20 meters, and the signal is contained by walls and windows. This feature has the advantage of isolating the transmission systems in different rooms. The system cannot operate outdoors.

The transmission system uses pulse-position modulation (PPM) in which the binary data is mapped into symbols that consist of a group of slots.



Infrared PLCP frame format

Figure shows the format of the PLCP frame. The PLCP preamble starts with a minimum of 57 and a maximum of 73 slots of alternating presence and absence of pulse in consecutive slots. The receiver uses this sequence to perform slot synchronization and other optional initialization procedures. The PLCP header consists of a 3 data rate field to indicate the data rate (000 for 1 Mbps; 001 for 2 Mbps); a 32 bit slot sequence of pulses that stabilizes the DC level of the received signal; a 16-bit integer that indicates the length of the PSDU; and a 16-bit CRC calculated over the length field using the CCITT-16 generator polynomial. The PSDU field consists of 0 to 2500 octets modulated using the L-PPM format. The PLCP length, CRC, and PSDU fields can be transmitted at either 1 Mbps or 2 Mbps. The fields prior to these are defined in terms of slots, not symbols.