UNIT 3

The Medium Access Control Sub Layer: The Channel Allocation Problem: Static Channel Allocation, Dynamic Channel Allocation.
Multiple Access Protocols: Aloha, pure ALOHA, Slotted ALOHA, CSMA: CSMA/CD, CSMA/CA, Collision Free Protocols, Limited Contention Protocols, Wireless LAN Protocols.
Ethernet: Classic Ethernet Physical Layer, Classic, MAC Sub-layer.
Wireless LAN'S: The 802.11 Architecture and Protocol Stack, The 802.11 Physical Layer,The802.11 MAC Sub-layer Protocol.

Introduction:

We know that two types of networks are there

1. Point-to-point
2. Broadcast Channels

The protocols used to determine who goes next on a multi-access channel belong to a Sub layer of the data link layer called the MAC sub layer.

The key issues are how to determine who gets to use the channel when there is competition for it.

For example, at a meeting, people raise their hands to request permission to speak. When only a single channel is available, determining who should go next is much harder. Many protocols for solving the problem are known and form the contents of this chapter. In the literature, broadcast channels are sometimes referred to as multi-access channels or random access channels.

The protocols used to determine who goes next on a multi-access channel belong to a sub layer of the data link layer called the MAC (Medium Access Control) Sub layer. The MAC Sub layer is especially important in LANs, many of which use a multi-access channel as the basis for communication. WANs, in contrast, use point-to-point links, except for satellite networks.

The Channel Allocation Problem

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.

Static Channel Allocation in LANs and MANs:

The traditional way of allocating a single channel among multiple competing users is Frequency Division Multiplexing (FDM).If there are N users, the bandwidth is divided into N equal-sized portions, each user being assigned one portion. Since each user has a private frequency band, there is no interference between users. When there is only a small and constant number of a user, each of which has a heavy (buffered) load of traffic (e.g., carriers' switching offices), FDM is a simple and efficient allocation mechanism. However, when the number of senders is large and continuously varying or the traffic is bursty, FDM presents some problems.

Dynamic Channel Allocation in LANs and MANs:

Frequency bands are not permanently assigned. Channels are allotted to users dynamically as needed from a central pool.

In this area are five key assumptions are there

Station Model: The model consists of N independent, each with a program or user that generates frames for transmission. Assumes that each of N stations independently produce frames. Stations are sometimes called terminals. Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

Single Channel Assumption: A single channel is available for all communication. All stations can transmit on it and all can receive from it.

Collision Assumption: If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is called a collision. All stations can detect collisions. A collided frame must be transmitted again later. There are no errors other than those generated by collisions.

4a. Continuous Time: Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.

4b. Slotted Time: Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

5a. Carrier Sense: Stations can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.

5b. No Carrier Sense: Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

Multiple Access Protocols

ALOHA

Aloha, also called the Aloha method, refers to a simple communications scheme in which each source (transmitter) in a network sends data whenever there is a frame to send. If the frame successfully reaches the destination (receiver), the next frame is sent. If the frame fails to be received at the destination, it is sent again.

Two versions of ALOHA here: pure and slotted. They differ with respect to whether time is divided into discrete slots into which all frames must fit. Pure ALOHA does not require global time synchronization; slotted ALOHA does.

Pure ALOHA

- It allows the stations to transmit data at any time whenever they want.
- After transmitting the data packet, station waits for some time.

Then, following 2 cases are possible-

Case-01:

- Transmitting station receives an acknowledgement from the receiving station.
- In this case, transmitting station assumes that the transmission is successful.

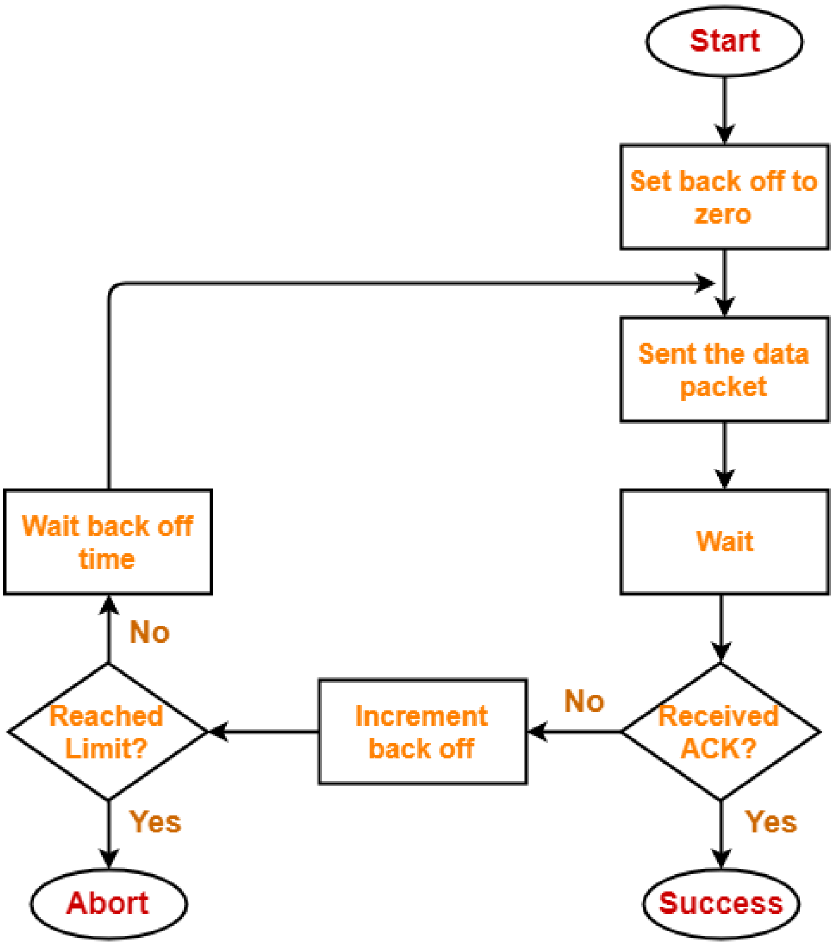
Case-02:

- Transmitting station does not receive any acknowledgement within specified time from the receiving station.
- In this case, transmitting station assumes that the transmission is unsuccessful.

Then,

- Transmitting station uses a **Back Off Strategy** and waits for some random amount of time.
- After back off time, it transmits the data packet again.
- It keeps trying until the back off limit is reached after which it aborts the transmission.

$$\boxed{\text{Efficiency of Pure Aloha } (\eta) = G \times e^{-2G}}$$



Advantages:

1. Superior to fixed assignment when there is a large number of bursty stations.
2. Adapts to varying number of stations.

Disadvantages:

1. Requires queuing buffers for retransmission of packets.

Slotted ALOHA

- Slotted Aloha divides the time of shared channel into discrete intervals called as **time slots**.
- Any station can transmit its data in any time slot.
- The only condition is that station must start its transmission from the beginning of the time slot.
- If the beginning of the slot is missed, then station has to wait until the beginning of the next time slot.
- A collision may occur if two or more stations try to transmit data at the beginning of the same time slot.

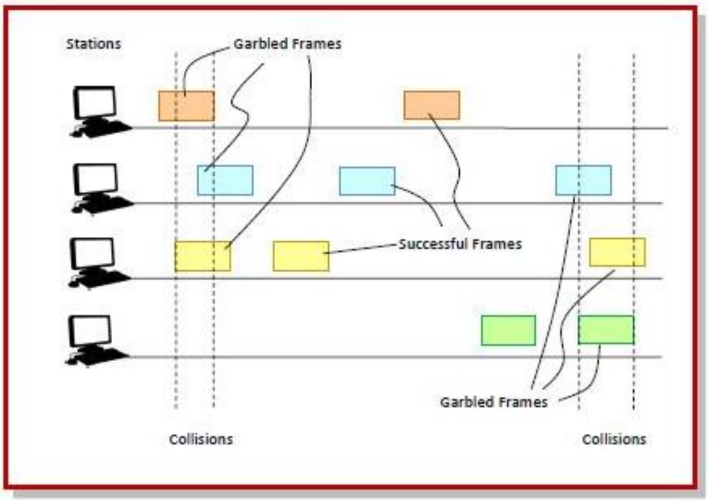
$$\text{Efficiency of Pure Aloha } (\eta) = G \times e^{-G}$$

Advantages:

1. Doubles the efficiency of Aloha.
2. Adaptable to a changing station population.

Disadvantages:

1. Requires queuing buffers for retransmission of packets.



Pure Aloha	Slotted Aloha
Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
Vulnerable time in which collision may occur = 2 x T_t	Vulnerable time in which collision may occur = T_t
Probability of successful transmission of data packet = G x e-^{2G}	Probability of successful transmission of data packet = G x e-^{G}
Maximum efficiency = 18.4%	Maximum efficiency = 36.8%
The main advantage of pure aloha is its simplicity in implementation.	The main advantage of slotted aloha is that it reduces the number of collisions to half and doubles the efficiency of pure aloha.

Carrier Sense Multiple Access (CSMA) Protocols

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

This access control method works as follows-

Step-01: Sensing the Carrier-

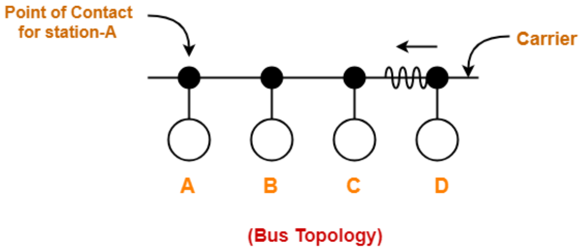
1. Any station willing to transmit the data senses the carrier.
2. If it finds the carrier free, it starts transmitting its data packet otherwise not

How?

- Each station can sense the carrier only at its point of contact with the carrier.
- It is not possible for any station to sense the entire carrier.
- Thus, there is a huge possibility that a station might sense the carrier free even when it is actually not.

Example-

Consider the following scenario-



At the current instance,

- If station A senses the carrier at its point of contact, then it will find the carrier free.
- But the carrier is actually not free because station D is already transmitting its data.
- If station A starts transmitting its data now, then it might lead to a collision with the data transmitted by station D.

Step-02: Detecting the Collision-

In CSMA / CD,

- It is the responsibility of the transmitting station to detect the collision.
- For detecting the collision, CSMA / CD implement the following condition.
- This condition is followed by each station-

Transmission delay >= 2 x Propagation delay

Two cases are possible-

Case-01:

If no collided signal comes back during the transmission,

- It indicates that no collision has occurred.

- The data packet is transmitted successfully.

<u>Case-02:</u>

If the collided signal comes back during the transmission,

- It indicates that the collision has occurred.
- The data packet is not transmitted successfully.
- Step-03 is followed.

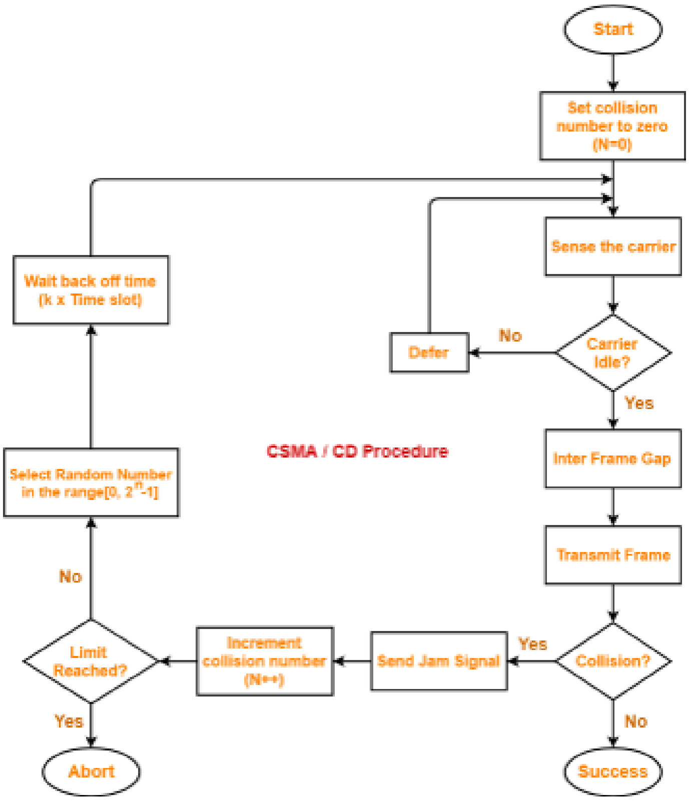
Step-03: Releasing Jam Signal-

- Jam signal is a 48 bit signal.
- It is released by the transmitting stations as soon as they detect a collision.
- It alerts the other stations not to transmit their data immediately after the collision.
- Otherwise, there is a possibility of collision again with the same data packet.
- Ethernet sends the jam signal at a frequency other than the frequency of data signals.
- This ensures that jam signal does not collide with the data signals undergone collision.

Step-04: Waiting For Back Off Time-

- After the collision, the transmitting station waits for some random amount of time called as **back off time**.
- After back off time, it tries transmitting the data packet again.
- If again the collision occurs, then station again waits for some random back off time and then tries again.
- The station keeps trying until the back off time reaches its limit.
- After the limit is reached, station aborts the transmission.
- Back off time is calculated using Back Off Algorithm.

CSMA / CD Flowchart-

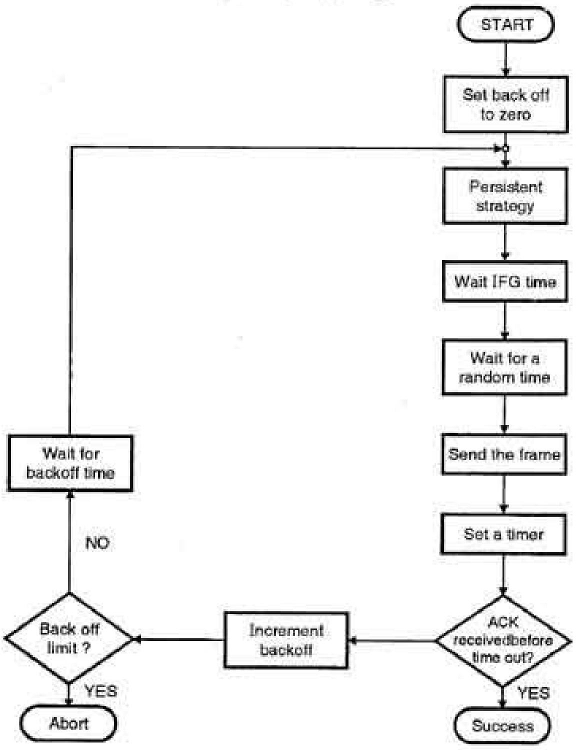


Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. In the case of wireless networks, most of the energy is used for transmission and the energy of the received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

These are three types of strategies:

1. **Inter Frame Space (IFS):** When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called **IFS time**. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
2. **Contention Window:** It is the amount of time divided into slots. A station that is ready to send frames chooses a random number of slots as **wait time**.
3. **Acknowledgments:** The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.



CSMA/CA procedure

Types of CSMA Access Modes:

There are 4 types of access modes available in CSMA. It is also referred as 4 different types of CSMA protocols which decides time to start sending data across a shared media.

1. **1-Persistent:** It senses the shared channel first and delivers the data right away if the channel is idle. If not, it must wait and ***continuously*** track for the channel to become idle and then broadcast the frame without condition as soon as it does. It is an aggressive transmission algorithm.
2. **Non-Persistent:** It first assesses the channel before transmitting data; if the channel is idle, the node transmits data right away. If not, the station must wait for an arbitrary amount of time (***not continuously***), and when it discovers the channel is empty, it sends the frames.
3. **P-Persistent:** It consists of the 1-Persistent and Non-Persistent modes combined. Each node observes the channel in the P-Persistent mode, and if the channel is idle, it sends a frame with a P probability. If

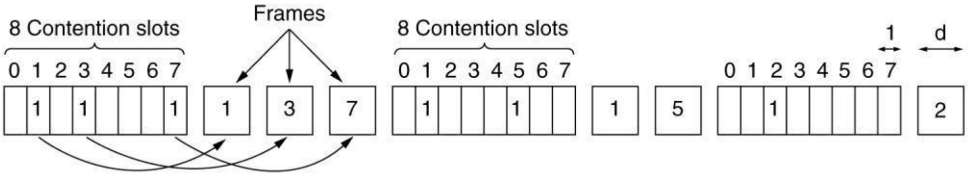
the data is not transferred, the frame restarts with the following time slot after waiting for a (q = 1-p probability) random period.

4. **0-Persistent:** A supervisory node gives each node a transmission order. Nodes wait for their time slot according to their allocated transmission sequence when the transmission medium is idle.

Collision-Free Protocols

A Bit-Map Protocol:

In our first collision-free protocol, the basic bit-map method, each contention period consists of exactly N slots. If station 0 has a frame to send, it transmits a 1 bit during the zeroth slot. No other station is allowed to transmit during this slot. Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 during slot 1, but only if it has a frame queued. In general, station j may announce that it has a frame to send by inserting a 1 bit into slot j. After all N slots have passed by, each station has complete knowledge of which stations wish to transmit. At that point, they begin transmitting in numerical order



Since everyone agrees on who goes next, there will never be any collisions. After the last ready station has transmitted its frame, an event all stations can easily monitor, another N bit contention period is begun. If a station becomes ready just after its bit slot has passed by, it is out of luck and must remain silent until every station has had a chance and the bit map has come around again. Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.

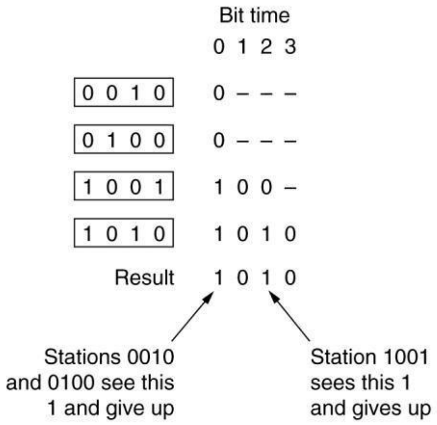
Binary Countdown

A problem with the basic bit-map protocol is that the overhead is 1 bit per station, so it does not scale well to networks with thousands of stations. We can do better than that by using binary station addresses. A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the high-order bit. All addresses are assumed to be the same length. The bits in each address position from different stations are BOOLEAN ORed together. We will call this protocol binary countdown.

It implicitly assumes that the transmission delays are negligible so that all stations see asserted bits essentially instantaneously.

To avoid conflicts, an arbitration rule must be applied: as soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up. For example, if stations 0010, 0100, 1001, and 1010 are all trying to get the channel, in the first bit time the stations transmit 0, 0, 1, and 1, respectively. These are ORed together to form a 1. Stations 0010 and 0100 see the 1 and know that a higher-numbered station is competing for the channel, so they give up for the current round. Stations 1001 and 1010 continue.

The next bit is 0, and both stations continue. The next bit is 1, so station 1001 gives up. The winner is station 1010 because it has the highest address. After winning the bidding, it may now transmit a frame, after which another bidding cycle starts. The protocol is illustrated in Fig. . It has the property that higher-numbered stations have a higher priority than lower-numbered stations, which may be either good or bad, depending on the context.



The binary countdown protocol. A dash indicates silence.

Limited Contention Protocols:

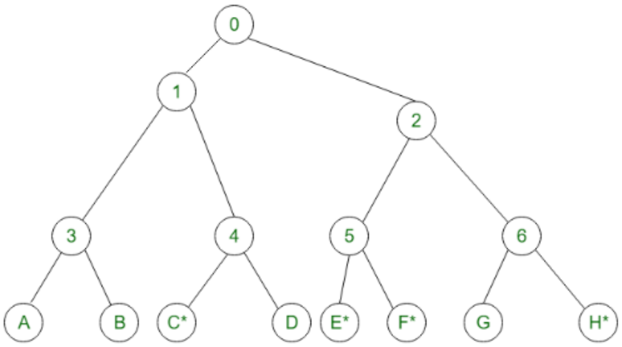
- Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
- Collision free protocols (bitmap, binary Countdown) are good when load is high.
- How about combining their advantages
  1. Behave like the ALOHA scheme under light load
  2. Behave like the bitmap scheme under heavy load.
- Limited contention protocols divide the contending stations into groups, which may or not be disjoint. At slot 0, only stations in group 0 can compete for channel access. At slot 1, only stations in group 1 can compete for channel access and so on. In this process, if a station successfully acquires the channel, then it transmits its data frame. If there is a collision or there are no stations competing for a given slot in a group, the stations of the next group can compete for the slot.
- By dynamically changing the number of groups and the number of stations allotted in a group according to the network load, the protocol changes from slotted ALOHA under low loads to bit map protocol under high loads. Under low loads, only one group is there containing all stations, which is the case of slotted ALOHA. As the load increases, more groups are added and the size of each group is reduced. When the load is very high, each group has just one station, i.e. only one station can compete at a slot, which is the case of bit map protocol.
- The performance of limited contention protocol is highly dependent upon the algorithm to dynamically adjust the group configurations to the changes in network environment

Example − An example of limited contention protocol is Adaptive Tree Walk Protocol.

Adaptive Tree Walk Protocol:

- Partition the group of station and limit the contention for each slot.
- Under light load, everyone can try for each slot like aloha
- Under heavy load, only a group can try for each slot
- **How do we do it:**

1. treat every stations as the leaf of a binary tree
2. first slot (after successful transmission), all stations can try to get the slot(under the root node).
3. if no conflict, fine
4. in case of conflict, only nodes under a subtree get to try for the next one. (depth first search)



- **Slot-0:** C*, E*, F*, H* (all nodes under node 0 can try which are going to send), conflict
- **Slot-1:** C* (all nodes under node 1can try}, C sends
- **Slot-2:** E*, F*, H*(all nodes under node 2 can try}, conflict
- **Slot-3:** E*, F* (all nodes under node 5 can try to send), conflict
- **Slot-4:** E* (all nodes under E can try), E sends
- **Slot-5:** F* (all nodes under F can try), F sends
- **Slot-6:** H* (all nodes under node 6 can try to send), H sends.

Wireless LAN Protocols:

Wireless LANs refer to LANs (Local Area Networks) that use high frequency radio waves instead of cables for connecting the devices. It can be conceived as a set of laptops and other wireless devices communicating by radio signals. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

Configuration of Wireless LANs

Each station in a Wireless LAN has a wireless network interface controller. A station can be of two categories −

- **Wireless Access Point (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access points. The APs are wired together using fiber or copper wires, through the distribution system.
- **Client** − Clients are workstations, computers, laptops, printers, smart phones etc. They are around tens of metres within the range of an AP.

Types of WLAN Protocols

IEEE 802.11 or WiFi has a number of variations, the main among which are −

- **802.11a Protocol**– This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).

- **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.

- **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.

- **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

Ethernet (IEEE 802.3)

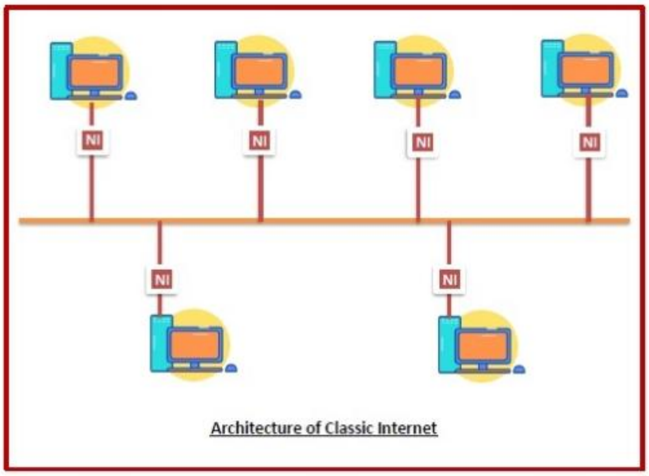
Classic Ethernet Physical Layer

Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used.

Architecture

Classic Ethernet is simplest form of Ethernet. It comprises of an Ethernet medium composed of a long piece of coaxial cable. Stations can be connected to the coaxial cable using a card called the network interface (NI). The NIs are responsible for receiving and transmitting data through the network. Repeaters are used to make end-to-end joins between cable segments as well as re-generate the signals if they weaken. When a station is ready to transmit, it places its frame in the cable. This arrangement is called the broadcast bus.

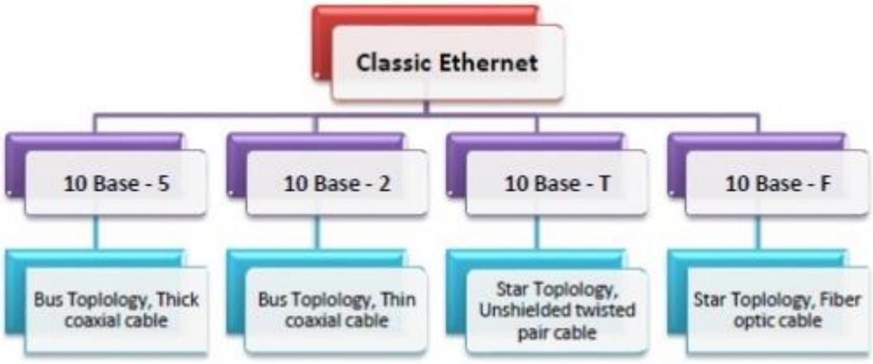
The configuration is illustrated as follows −

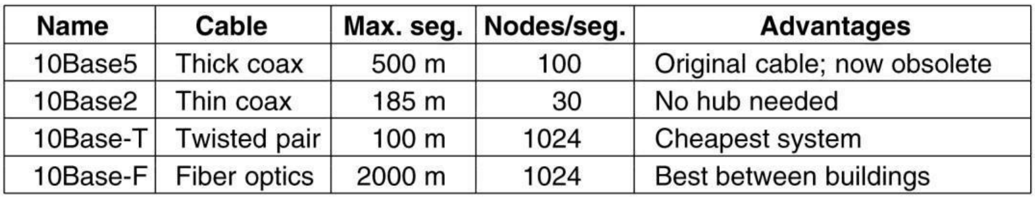


Varieties of Classic Ethernet

The common varieties of classic Ethernet are -

- Thick coax (10BASE-5): This was the original version that used a single coaxial cable into which a connection can be tapped by drilling into the cable to the core. The 5 refers to the maximum segment length of 500m.
- Thin coax (10BASE-2): This is a thinner variety where segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- Twisted pair (10BASE-T): This uses unshielded twisted pair copper wires as physical layer medium.
- Ethernet over Fiber (10BASE-F): This uses fiber optic cables as medium of transmission.

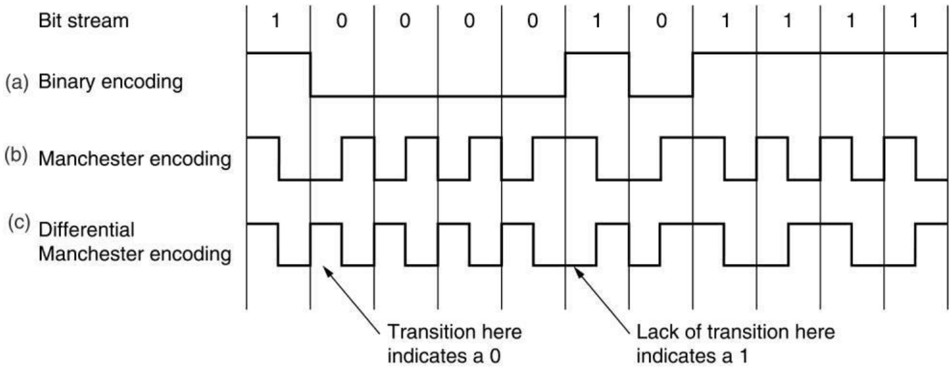

Classic Ethernet
10 Base - 5
10 Base - 2
10 Base - T
10 Base - F
Bus Toplology, Thick coaxial cable
Bus Toplology, Thin coaxial cable
Star Toplology, Unshielded twisted pair cable
Star Toplology, Fiber optic cable



Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Manchester Encoding

Two approaches called Manchester encoding and differential Manchester encoding. With Manchester encoding, each bit period is divided into two equal intervals. A binary 1 bit is sent by having the voltage set high during the first interval and low in the second one. A binary 0 is just the reverse: first low and then high. This scheme ensures that every bit period has a transition in the middle, making it easy for the receiver to synchronize with the sender. A disadvantage of Manchester encoding is that it requires twice as much bandwidth as straight binary encoding because the pulses are half the width. For example, to send data at 10 Mbps, the signal has to change 20 million times/sec. Manchester encoding is shown in Fig.

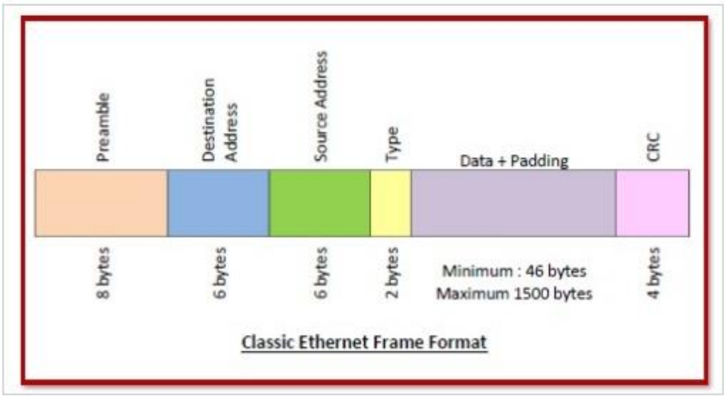

Bit stream
1 0 0 0 0 1 0 1 1 1 1
(a) Binary encoding
(b) Manchester encoding
(c) Differential Manchester encoding
Transition here indicates a 0
Lack of transition here indicates a 1

The Ethernet MAC Sublayer

Frame Format of Classic Ethernet

The main fields of a frame of classic Ethernet are −

- Preamble: It is a 8 bytes starting field that provides alert and timing pulse for transmission.
- Destination Address: It is a 6 byte field containing physical address of destination stations.
- Source Address: It is a 6 byte field containing the physical address of the sending station.
- Type: It a 2 bytes field that instructs the receiver which process to give the frame to.
- Data: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- Padding: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- CRC: CRC stands for cyclic redundancy check. It contains the error detection information.



Wireless LAN's

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

The 802.11 architecture and protocol stack

802.11 networks can be used in two modes: infrastructure mode and ad-hoc mode

Infrastructure mode uses an AP (Access Point) that is connected to the network. Clients send and receive packets via the AP. Several APs can be connected to form an extended network

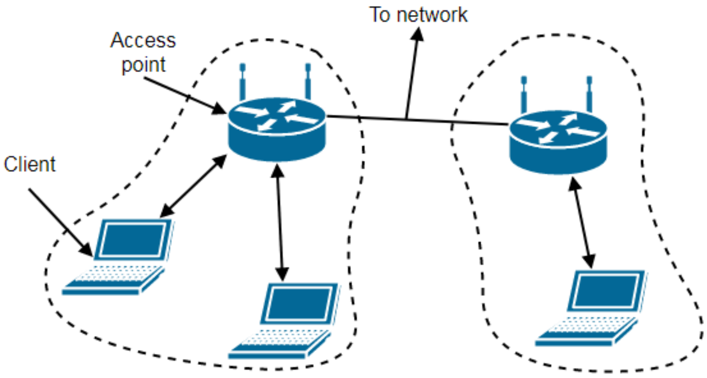


Fig. Architecture in Infrastructure mode

Ad-hoc mode is a collection of computers connected to each other so that they can send frames to each other. There's no AP

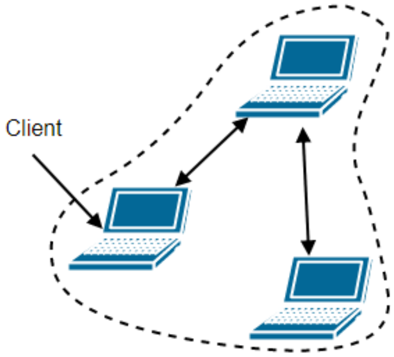
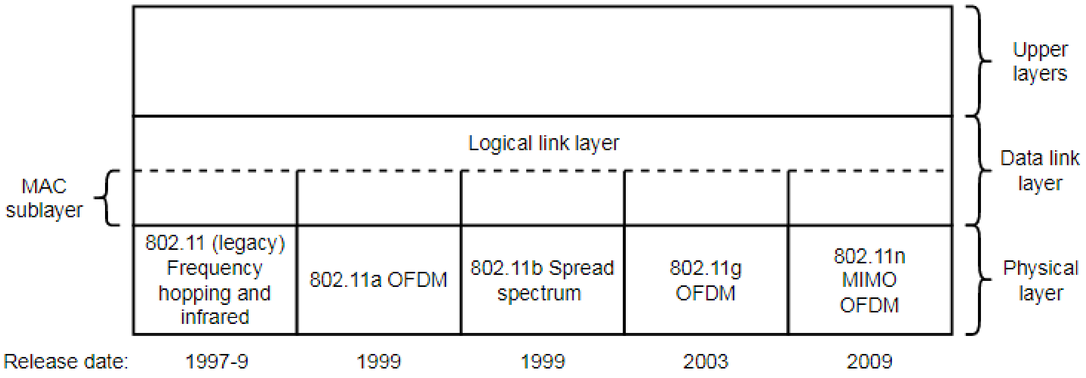


Fig. Architecture in Ad-hoc mode

The 802.11 physical layer corresponds to the OSI physical layer, but the data link layer is split into multiple sub layers.



In 802.11 the MAC sublayer determines which channel gets to transmit next. The sublayer above, the LLC (Logical Link Layer), hides the differences between the varying 802.11 versions for the network layer .

The 802.11 physical layer

All 802.11 techniques use short-range radios to transmit signals in either 2.4-GHz or 5-GHz ISM frequency bands”. These bands are unlicensed, and so are shared by many other devices such as garage door openers, or microwave ovens. Fewer applications tend to use the 5-GHz band, so 5-GHz can be better for some applications despite shorter range due to higher frequency.

All 802.11 transmission methods define multiple rates. Different rates can be used depending on the current conditions. If the signal is weak, a low rate is used. If the signal is clear, the highest rate is used. The process of adjustment is called **rate adaption**.

The infrared option uses diffused (i.e., not line of sight) transmission at 0.85 or 0.95 microns. Two speeds are permitted: 1 Mbps and 2 Mbps. At 1 Mbps, an encoding scheme is used in which a group of 4 bits is encoded as a 16-bit codeword containing fifteen 0s and a single 1, using what is called Gray code. This code has the property that a small error in time synchronization leads to only a single bit error in the output. At 2 Mbps, the encoding takes 2 bits and produces a 4-bit codeword, also with only a single 1, that is one of 0001, 0010, 0100, or 1000. Infrared signals cannot penetrate walls, so cells in different rooms are well isolated from each other. Nevertheless, due to the low bandwidth (and the fact that sunlight swamps infrared signals), this is not a popular option.

FHSS (Frequency Hopping Spread Spectrum) uses 79 channels, each 1-MHz wide, starting at the low end of the 2.4-GHz ISM band. A pseudorandom number generator is used to produce the sequence of frequencies hopped to. As long as all stations use the same seed to the pseudorandom number generator and stay synchronized in time, they will hop to the same frequencies simultaneously. The amount of time spent at each frequency, the dwell time, is an adjustable parameter, but must be less than 400 msec. FHSS' randomization provides a fair way to allocate spectrum in the unregulated ISM band. It also provides a modicum of security since an intruder who does not know the hopping sequence or dwell time cannot eavesdrop on transmissions. Over longer distances, multipath fading can be an issue, and FHSS offers good resistance to it. It is also relatively insensitive to radio interference, which makes it popular for building-to-building links. Its main disadvantage is its low bandwidth.

The third modulation method, DSSS (Direct Sequence Spread Spectrum), is also restricted to 1 or 2 Mbps. Each bit is transmitted as 11 chips, using what is called a Barker sequence. It uses phase shift modulation at 1 Mbaud, transmitting 1 bit per baud when operating at 1 Mbps and 2 bits per baud when operating at 2 Mbps. For years, the FCC required all wireless communications equipment operating in the ISM bands in the U.S. to use spread spectrum, but in May 2002, that rule was dropped as new technologies emerged.

The first of the high-speed wireless LANs, 802.11a, uses OFDM (Orthogonal Frequency Division Multiplexing) to deliver up to 54 Mbps in the wider 5-GHz ISM band. As the term FDM suggests, different frequencies are used—52 of them, 48 for data and 4 for synchronization—not unlike ADSL. Since transmissions are present on multiple frequencies at the same time, this technique is considered a form of spread spectrum, but different from both CDMA and FHSS. Splitting the signal into many narrow bands has some key advantages over using a single wide band, including better immunity to narrowband interference and the possibility of using noncontiguous bands. A complex encoding system is used, based on phase-shift modulation for speeds up to 18 Mbps and on QAM above that. At 54 Mbps, 216 data bits are encoded into 288-bit symbols. Part of the motivation for OFDM is compatibility with the European HiperLAN/2 system (Doufexi et al., 2002). The technique has a good spectrum efficiency in terms of bits/Hz and good immunity to multipath fading.

Next, we come to HR-DSSS (High Rate Direct Sequence Spread Spectrum), another spread spectrum technique, which uses 11 million chips/sec to achieve 11 Mbps in the 2.4-GHz band. It is called 802.11b but is not a follow-up to 802.11a. In fact, its standard was approved first and it got to market first. Data rates supported by 802.11b are 1, 2, 5.5, and 11 Mbps. The two slow rates run at 1 Mbaud, with 1 and 2 bits per baud, respectively, using phase shift modulation (for compatibility with DSSS). The two faster rates run at 1.375 Mbaud, with 4 and 8 bits per baud, respectively, using Walsh/Hadamard codes. The data rate may be dynamically adapted during operation to achieve the optimum speed possible under current conditions of load and noise. In practice, the operating speed of 802.11b is nearly always 11 Mbps. Although 802.11b is slower than 802.11a, its range is about 7 times greater, which is more important in many situations.

An enhanced version of 802.11b, 802.11g, was approved by IEEE in November 2001 after much politicking about whose patented technology it would use. It uses the OFDM modulation method of 802.11a but operates in the narrow 2.4-GHz ISM band along with 802.11b. In theory it can operate at up to 54 MBps. It is not yet clear whether this speed will be realized in practice. What it does mean is that the 802.11 committee has produced three different high-speed wireless LANs: 802.11a, 802.11b, and 802.11g (not to mention three low-speed wireless LANs). One can legitimately ask if this is a good thing for a standards committee to do. Maybe three was their lucky number.

The 802.11 MAC Sublayer Protocol

The 802.11 MAC sublayer is different from the Ethernet MAC sublayer for two reasons:

- Radios are almost always half duplex
- Transmission ranges of different stations might be different

802.11 uses the CSMA/CA (CSMA with Collision Avoidance) protocol. CSMA/CA is similar to ethernet CSMA/CD. It uses channel sensing and exponential backoff after collisions, but instead of entering backoff once a collision has been detected, CSMA/CA uses backoff immediately (unless the sender has not used the channel recently and the channel is idle)

The algorithm will backoff for a number of slots, for example 0 to 15 in the case of the of the OFDM physical layer. The station waits until the channel is idle by sensing that there is no signal for a short period of time. It counts down idle slots, pausing when frames are sent. When its counter reaches 0, it sends its frames.

Acknowledgements “are used to infer collisions because collisions cannot be detected” .

This way of operating is called DCF (Distributed Coordination Function). in DCF each station is acting independently, without a central control.

The other problem facing 802.11 protocols is transmission ranges differing between stations. It's possible for transmissions in one part of a cell to not be received in another part of the cell, which can make it impossible for a sender to sense a busy channel, resulting in collisions.

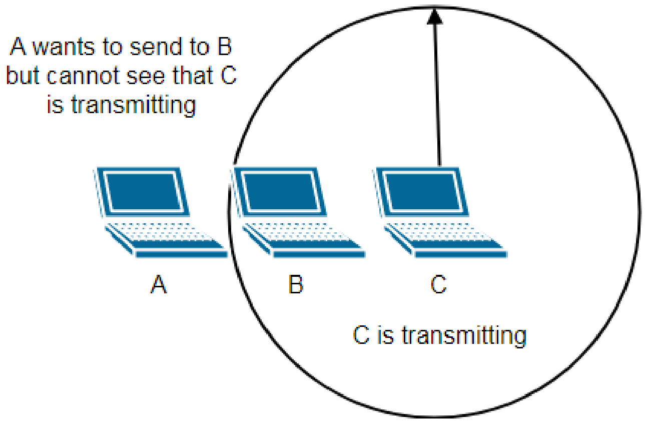


Figure: The hidden terminal problem

802.11 defines channel sensing to consist of physical and virtual sensing. Physical sensing "checks the medium to see if there is a valid signal".

With virtual sensing, each station keeps a record of what channel is in use. It does this with the NAV (Network Allocation Vector). Each frame includes a NAV field that contains information on how long the sequence that the frame is part of will take to complete.

802.11 is designed to:

- Be reliable.
- Be power-saving.
- Provide quality of service.

The main strategy for reliability is to lower the transmission rate if too many frames are unsuccessful. Lower transmission rates use more robust modulations. If too many frames are lost, a station can lower its rate. If frames are successfully delivered, a station can test a higher rate to see if should upgrade .

Another strategy for successful transmissions is to send shorter frames. 802.11 allows frames to be split into fragments, with their own checksum. The fragment size can be adjusted by the AP. Fragments are numbered and sent using a stop-and-wait protocol .

802.11 uses beacon frames. Beacon frames are broadcast periodically by the AP. The frames advertise the presence of the AP to clients and carry system parameters, such as the identifier of the AP, the time, how long until the next beacon, and security settings" .

Clients can set a power-management bit in frames that are sent to the AP to alert it that the client is entering power-save mode. In power-save mode, the client rests and the AP buffers traffic intended for it. The client wakes up for every beacon, and checks a traffic map that's sent with the beacon. The traffic map tells the client whether there is buffered traffic. If there is, the client sends a poll to the AP, and the AP sends the buffered traffic .

802.11 provides quality of service by extending CSMA/CA with defined intervals between frames. Different kinds of frames have different time intervals. The interval between regular data frame is called the DIFS (DCF InterFrame Spacing). Any station can attempt to acquire a channel after the channel has been idle for DIFS .

The shortest interval is SIFS (Short InterFrame Spacing). SIFS is used to send an ACK, other control frames like RTS, or for sending another fragment (which prevents another station from transmitting during the middle of a frames.

Different priorities of traffic are determined with different AIFS (Arbitration InterFrame Space) intervals. A short AIF can allow the AP to send higher priority traffic. An AIF that is longer than DIFS means the traffic will be sent after regular traffic.

Another quality of service mechanism is transmission opportunity. Previously, CSMA/CA allowed only one frame to be sent at a time. This slowed down stations with significantly faster rates. Transmission opportunities make it so each station has equal airtime, not an equal number of sent frames.

802.11 frame structure
There are three different classes of frames used in the air:

- Data
- Control
- Management

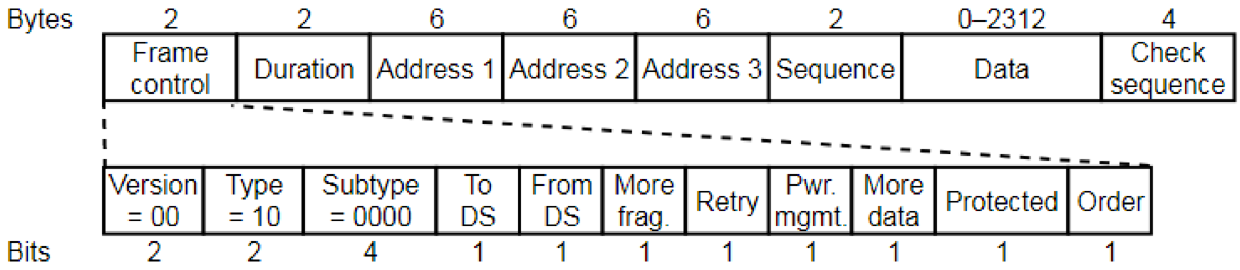


Figure: Format of the 802.11 data frame

The first part of frame is the *Frame Control* field, made up of 11 subfields:

- *Protocol Version*: set to 00 for current versions of 802.11.
- *Type*: can be one of data, control, or management, and the *Subtype* (e.g RTS or CTS). These are set to 10 and 0000 in binary for a normal data field.
- *To DS* and *From DS*: these bits indicate whether frames are coming or going from a network connected to the AP (the network is called the distribution system).
- *More Fragments*: this bit means that more fragments will follow.
- *Retry*: this bit “marks a retransmission of a frame sent earlier”.
- *Power Management*: this bit indicates that the sender is going into power-save mode.
- *More Data*: this bit indicates that the sender has additional frames for the receiver.
- *Protected Frame*: this bit indicates that the frame body has been encrypted for security.
- *Order*: this “bit tells the receiver that the higher layer expects the sequence of frames to arrive strictly in order”.

The second field in the data frame is the *Duration* field. This describes how long the frame and its acknowledgements will occupy the channel (measured in microseconds). It’s included in all frames, including control frames.

The addresses to and from an AP follow the standard IEEE 802 format. The *Address 1* is the receiver, *Address 2* is the transmitter, *Address 3* is the address of the endpoint that originally sent the frame via the AP.

The *Sequence* 16-bit field numbers frames so that duplicates can be detected. The first 4 bits identify the fragment, the last 12 contain a number that’s incremented on each transmission.

The *Data* field contains the payload. It can be up to 2312 bytes. The first bytes of the payload are for the LLC layer to identify the higher-layer protocol that the data is a part of.

The final part of the frame is the *Frame Check Sequence* field, containing a 32-bit CRC for validating the frame.

"Management frames have the same format as data frames, plus a format for the data portion that varies with the subtype (e.g. parameters in beacon frames)".

Control frames contain *Frame Control*, *Duration*, and *Frame Check Sequence* fields, but they might only have one address and no *Data* section.

Services

The 802.11 standard states that each conformant wireless LAN must provide nine services. These services are divided into two categories: five distribution services and four station services. The distribution services relate to managing cell membership and interacting with stations outside the cell. In contrast, the station services relate to activity within a single cell.

The five distribution services are provided by the base stations and deal with station mobility as they enter and leave cells, attaching themselves to and detaching themselves from base stations. They are as follows.

1. **Association**. This service is used by mobile stations to connect themselves to base stations. Typically, it is used just after a station moves within the radio range of the base station. Upon arrival, it announces its identity and capabilities. The capabilities include the data rates supported, need for PCF services (i.e., polling), and power management requirements. The base station may accept or reject the mobile station. If the mobile station is accepted, it must then authenticate itself.
2. **Disassociation.** Either the station or the base station may disassociate, thus breaking the relationship. A station should use this service before shutting down or leaving, but the base station may also use it before going down for maintenance.
3. **Reassociation.** A station may change its preferred base station using this service. This facility is useful for mobile stations moving from one cell to another. If it is used correctly, no data will be lost as a consequence of the handover. (But 802.11, like Ethernet, is just a best-efforts service.)
4. **Distribution.** This service determines how to route frames sent to the base station. If the destination is local to the base station, the frames can be sent out directly over the air. Otherwise, they will have to be forwarded over the wired network.
5. **Integration.** If a frame needs to be sent through a non-802.11 network with a different addressing scheme or frame format, this service handles the translation from the 802.11 format to the format required by the destination network.

The remaining four services are intracell (i.e., relate to actions within a single cell). They are used after association has taken place and are as follows.

1. **Authentication**. Because wireless communication can easily be sent or received by unauthorized stations, a station must authenticate itself before it is permitted to send data. After a mobile station has been associated by the base station (i.e., accepted into its cell), the base station sends a special challenge frame to it to see if the mobile station knows the secret key (password) that has been assigned to it. It proves its knowledge of the secret key by encrypting the challenge frame and sending it back to the base station. If the result is correct, the mobile is fully enrolled in the cell. In the initial standard, the base station does not have to prove its identity to the mobile station, but work to repair this defect in the standard is underway.
2. **Deauthentication.** When a previously authenticated station wants to leave the network, it is deauthenticated. After deauthentication, it may no longer use the network.
3. **Privacy.** For information sent over a wireless LAN to be kept confidential, it must be encrypted. This service manages the encryption and decryption. The encryption algorithm specified is RC4, invented by Ronald Rivest of M.I.T.
4. **Data delivery.** Finally, data transmission is what it is all about, so 802.11 naturally provides a way to transmit and receive data. Since 802.11 is modeled on Ethernet and transmission over Ethernet is not guaranteed to be 100% reliable, transmission over 802.11 is not guaranteed to be reliable either. Higher layers must deal with detecting and correcting errors.