Course Material

|  |  |  |  |
| --- | --- | --- | --- |
| **Course Material** | | | |
| **Department of Computer Science & Engineering** | | | |
| Course Code: |  | Semester: | VI |
| Course Title: | COMPUTER NETWORKS | Year: | 2021-2022 |
| Faculty Name: |  | | |

DAYANANDA SAGAR UNIVERSITY

School of Engineering, Innovation Campus,

Kudlu Gate, Hosur Road, Bengaluru 50068

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | | |
|  |  | | | | | |
|  |  | | | | | |
|  |  | | | | | |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |



|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
|  |  |  |  |
|  |  |  |  |



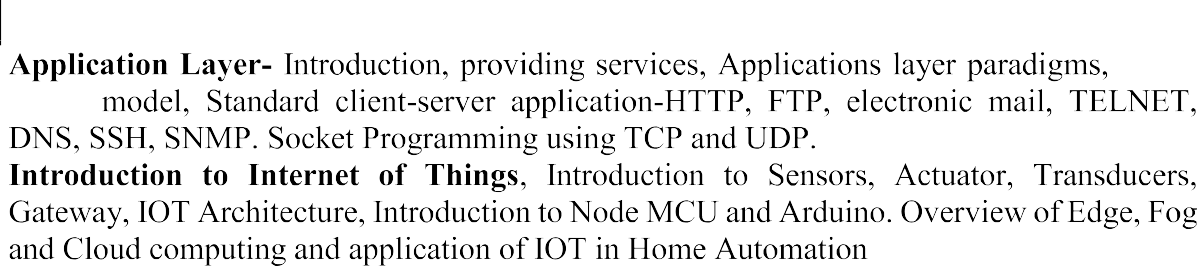
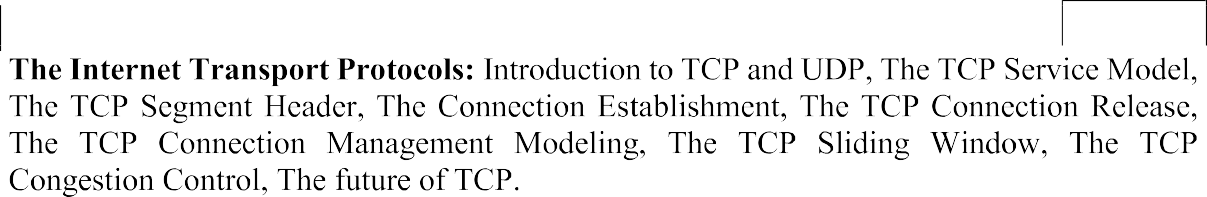






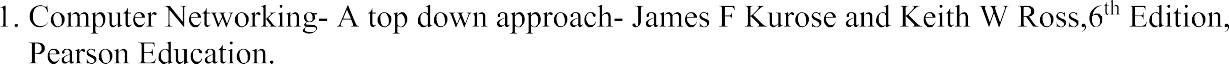
|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
|  | |
|  |  |
|  | |
|  |  |
|  |  |
|  | |









Data Link Layer

The [data link layer](https://www.javatpoint.com/data-link-layer) is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as [**media access control**](https://www.javatpoint.com/mac-full-form) or the multiple access resolutions.

Data Link Control

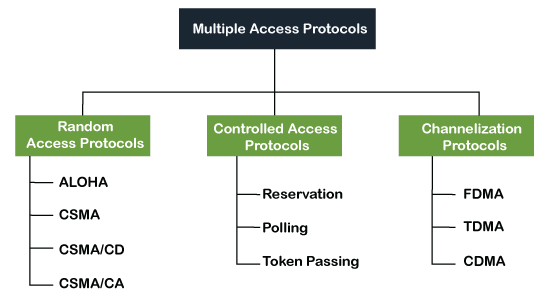
A [data link control](https://www.javatpoint.com/data-link-controls) is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore, it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Following are the types of multiple access protocol that is subdivided into the different process as:



### **A. Random Access Protocol**

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

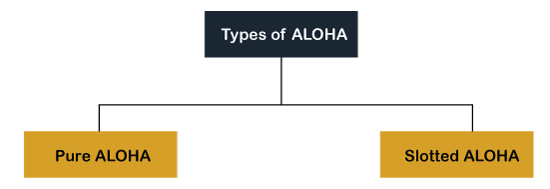
* Aloha
* CSMA
* CSMA/CD
* CSMA/CA

### **ALOHA Random Access Protocol**

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

**Aloha Rules**

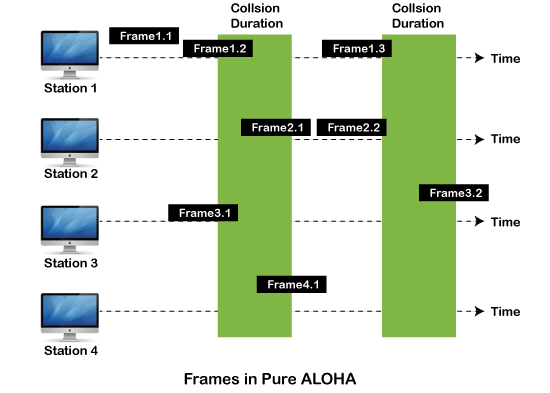
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



**Pure Aloha**

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 \* Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G \* e ^ - 2 G.

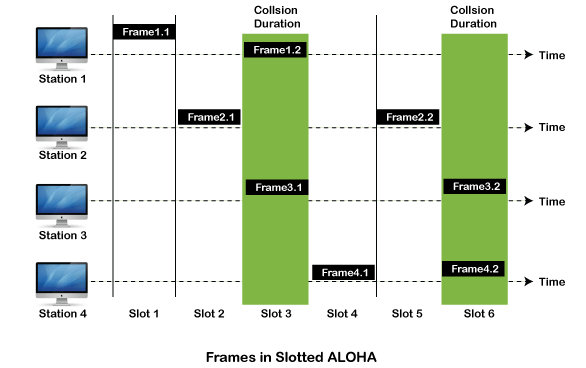


As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

**Slotted Aloha**

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G \* e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



### **CSMA (Carrier Sense Multiple Access)**

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

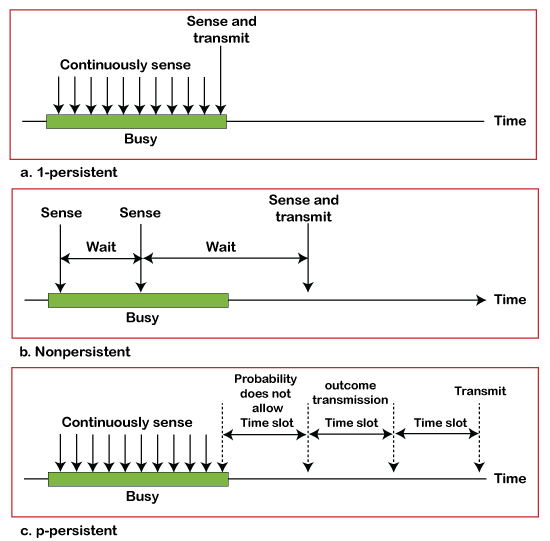
**CSMA Access Modes**

**1-Persistent:** In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

**Non-Persistent:** It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

**P-Persistent:** It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

**O- Persistent:** It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



### **CSMA/ CD**

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

### **CSMA/ CA**

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgment, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the [CSMA/ CA](https://www.javatpoint.com/csma-ca-vs-csma-cd) to avoid the collision:

**Interframe space**: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

**Contention window**: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

**Acknowledgment**: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

### **B. Controlled Access Protocol**

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

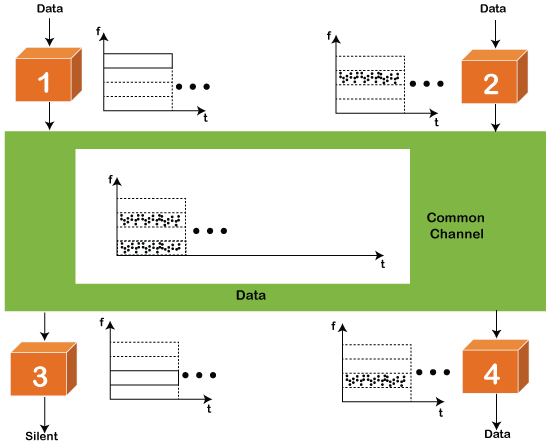
### **C. Channelization Protocols**

It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)

**FDMA**

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.

**TDMA**

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

**CDMA**

The [code division multiple access (CDMA)](https://www.javatpoint.com/cdma-full-form) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

**ETHERNET:**

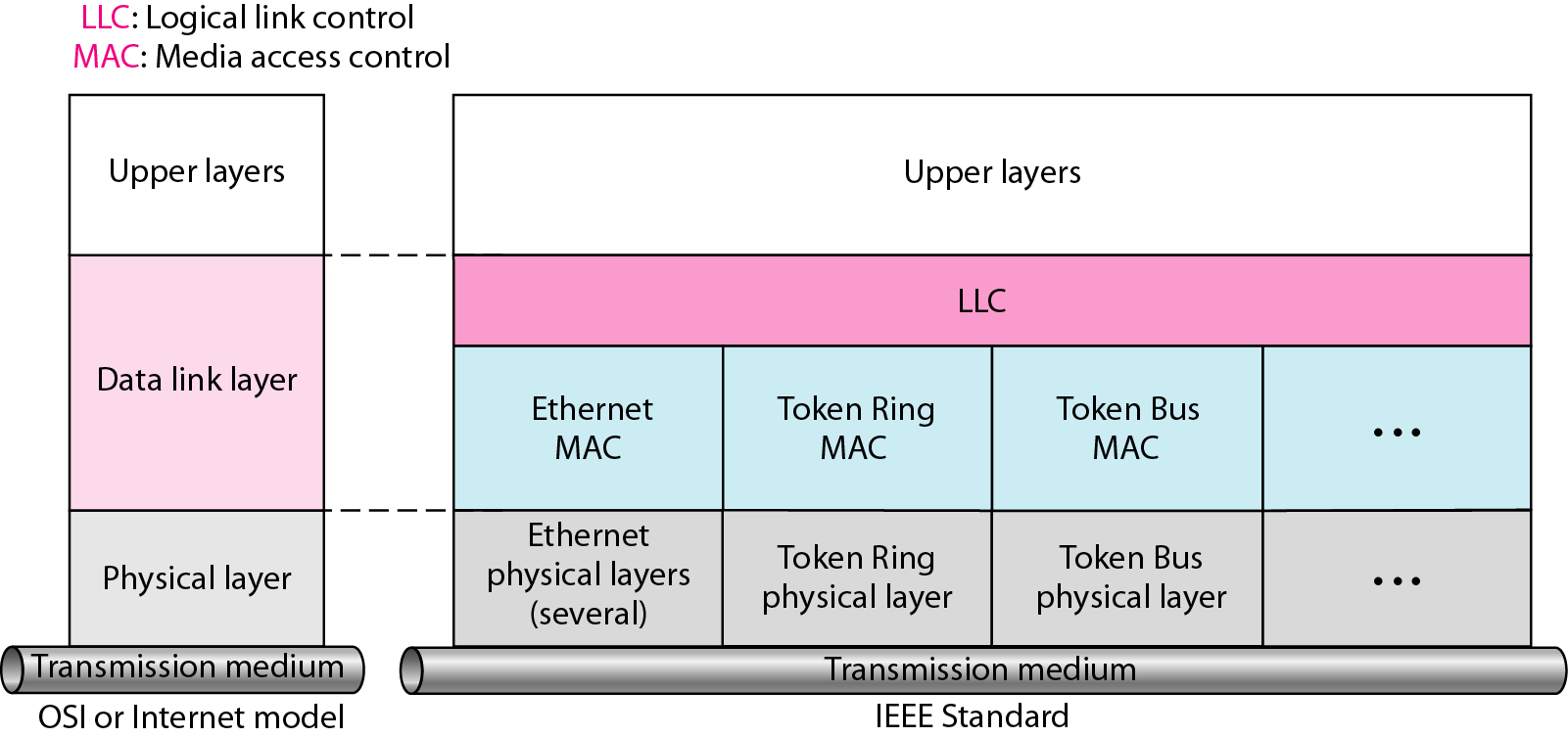
**IEEE STANDARDS**

The LAN market has several technologies such as Ethernet, Token Ring, Token Bus, FDDI, and ATM LAN.

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

**Figure *IEEE standard for LANs***

**The IEEE has subdivided data link layer into two sublayers: logical link control (LLC) and media access control (MAC).**



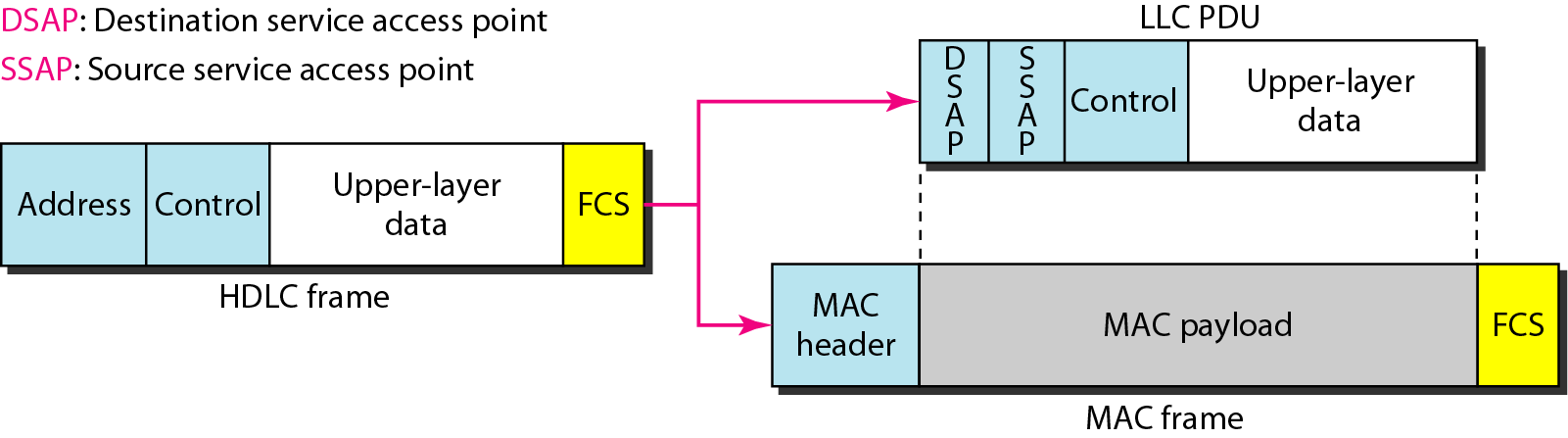
**Logical Link Control**

* In IEEE Project 802, flow control, error control and part of framing duties are collected into one sublayer called the logical link control.
* The LLC provides one single data link control protocol for all IEEE LANs.
* A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent**.**

**Framing:**

* LLC defines a Protocol data unit (PDU) has the header field which is used for flow and error control.
* The two other header fields define the upper-layer protocol at the source and destination that uses LLC – destination service access point and source service access point.

**Figure *HDLC frame compared with LLC and MAC frames***



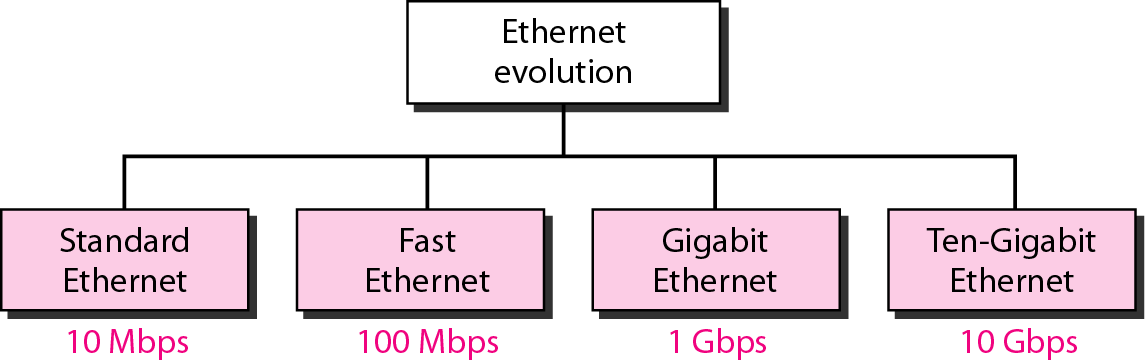
**Medium Access Control:**

* It specifies the media access method for each LAN.
* For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token-passing method for Token Ring and Token Bus LANs.
* It defines the access method and the framing format specific to corresponding LAN protocol.

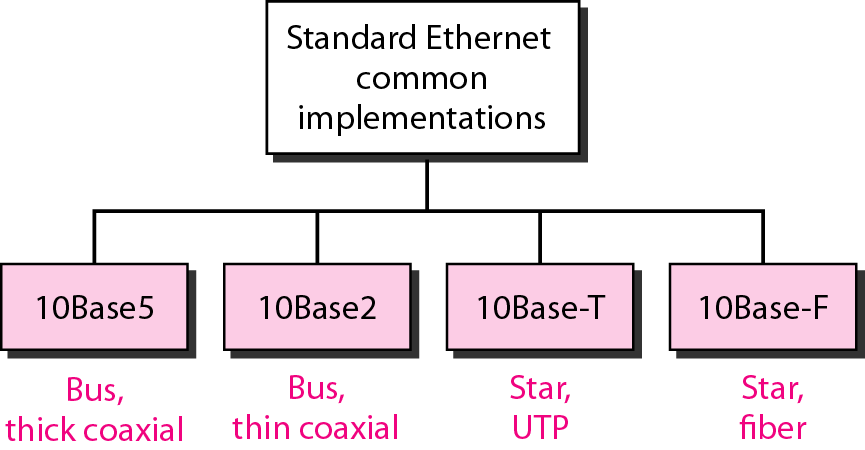
**STANDARD ETHERNET:**

The original Ethernet was created in 1976 at Xerox’s Palo Alto Research Center (PARC). Since then, it has gone through four generations. We briefly discuss the Standard (or traditional) Ethernet in this section.

**Figure *Ethernet evolution through four generations***



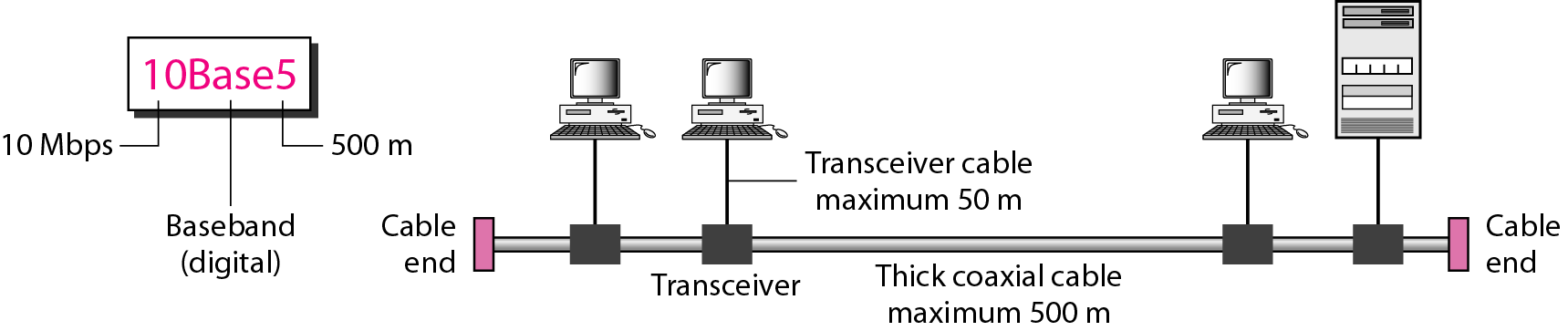
**Figure *Categories of Standard Ethernet***



**lOBase5: Thick Ethernet**

* The first implementation is called 10BaseS, thick Ethernet, or Thicknet.
* The nickname derives from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands.
* lOBaseS was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable.

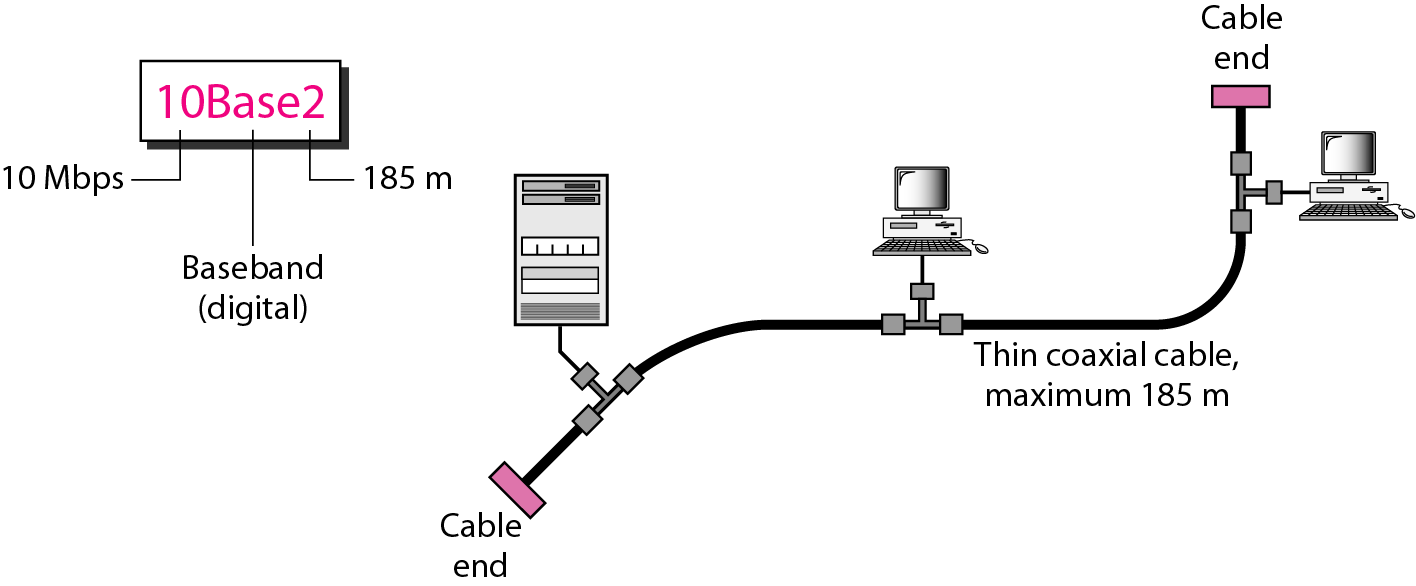
**Figure 13.10 *10Base5 implementation***



**10Base2: Thin Ethernet**

* The second implementation is called lOBase2, thin Ethernet, or Cheaper net. IOBase2 also uses a bus topology, but the cable is much thinner and more flexible.
* The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

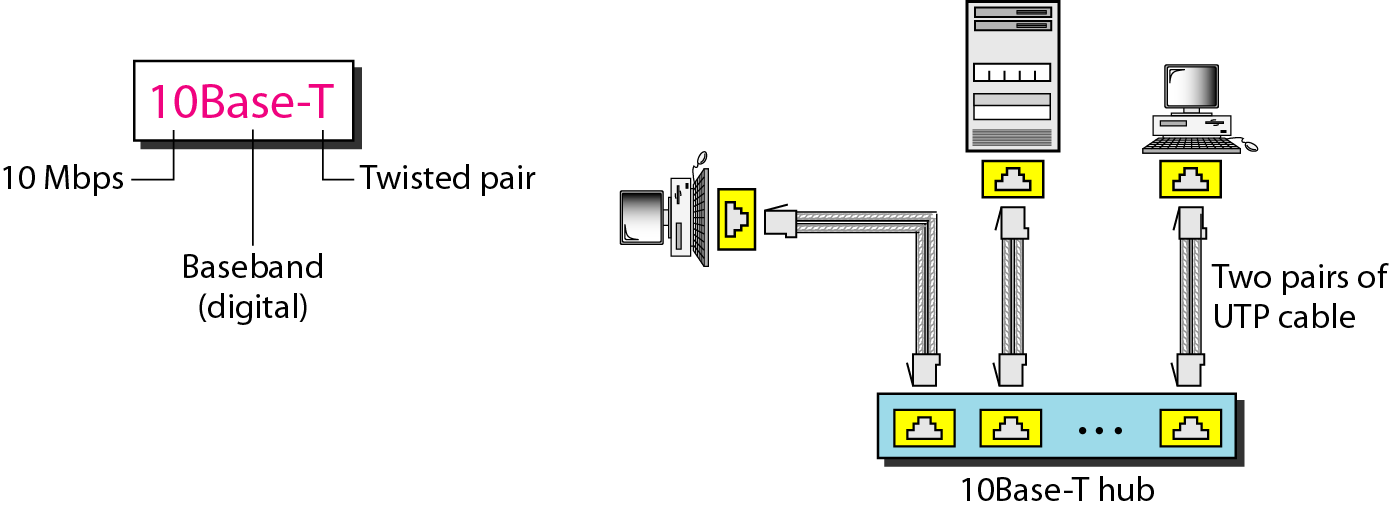
**Figure 13.11 *10Base2 implementation***



**lOBase-T: Twisted-Pair Ethernet**

The third implementation is called lOBase-T or twisted-pair Ethernet. 1OBase-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable, as shown in Figure 13.12

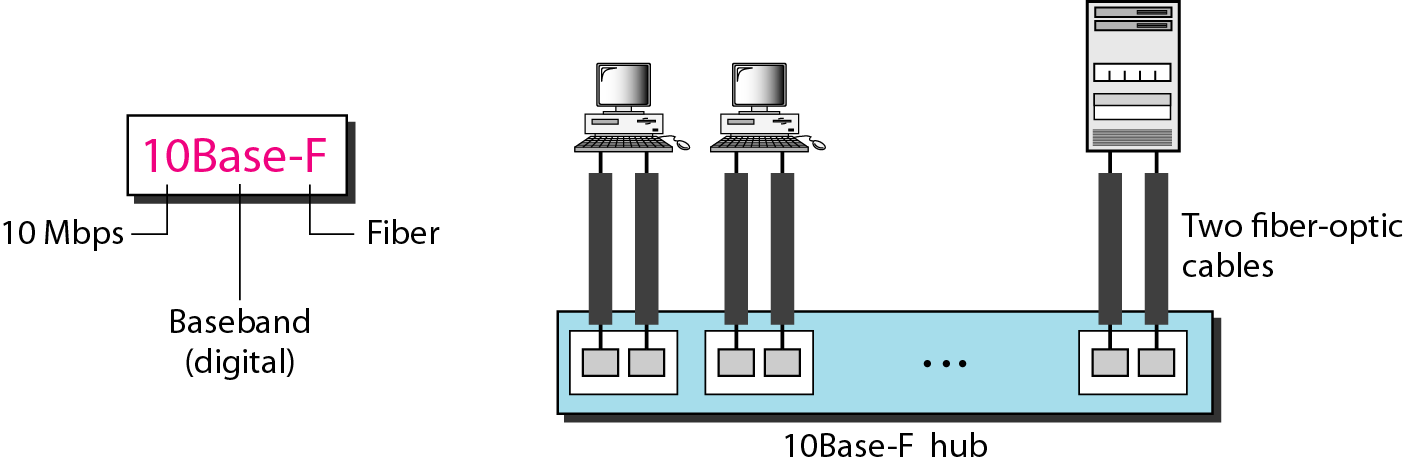
**Figure 13.12 *10Base-T implementation***



**lOBase-F: Fiber Ethernet**

* Although there are several types of optical fiber lO-Mbps Ethernet, the most common is called 10Base-F. lOBase-F uses a star topology to connect stations to a hub.
* The stations are connected to the hub using two fiber-optic cables, as shown in Figure 13.13.

**Figure 13.13 *10Base-F implementation***



**FAST ETHERNET:**

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.

The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.

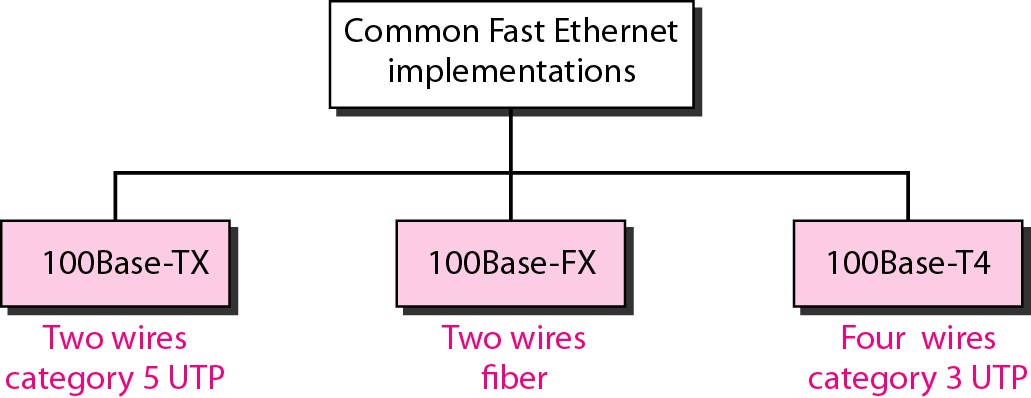
2. Make it compatible with Standard Ethernet.

3. Keep the same 48-bit address.

4. Keep the same frame format.

5. Keep the same minimum and maximum frame lengths

**Figure *Fast Ethernet implementations***



**GIGABIT ETHERNET:**

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z.

The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1 Gbps.

2. Make it compatible with Standard or Fast Ethernet.

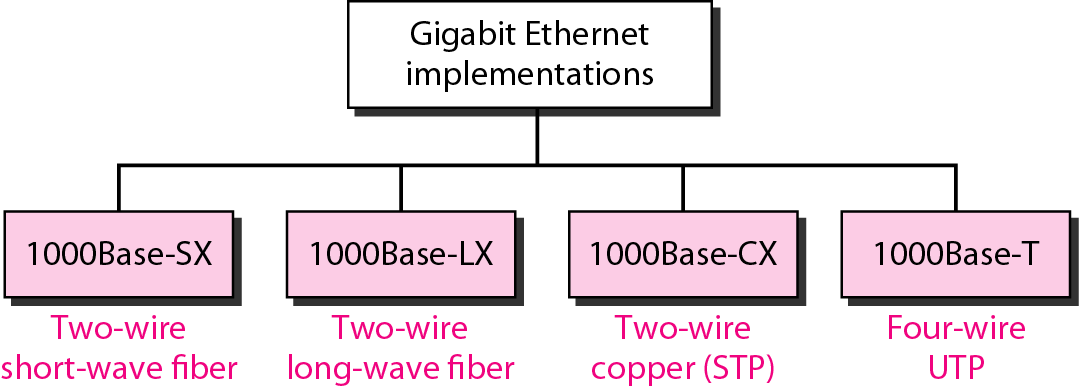
3. Use the same 48-bit address.

4. Use the same frame format.

5. Keep the same minimum and maximum frame lengths.

6. To support auto negotiation as defined in Fast Ethernet.

**Figure *Gigabit Ethernet implementations***

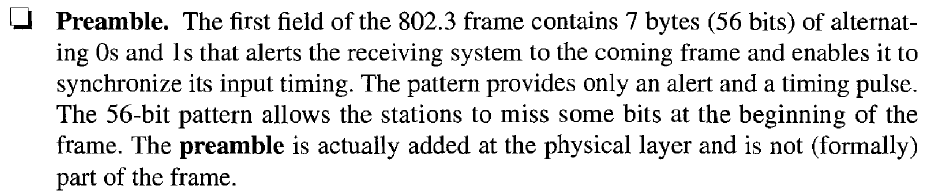


**MAC SUBLAYER:**

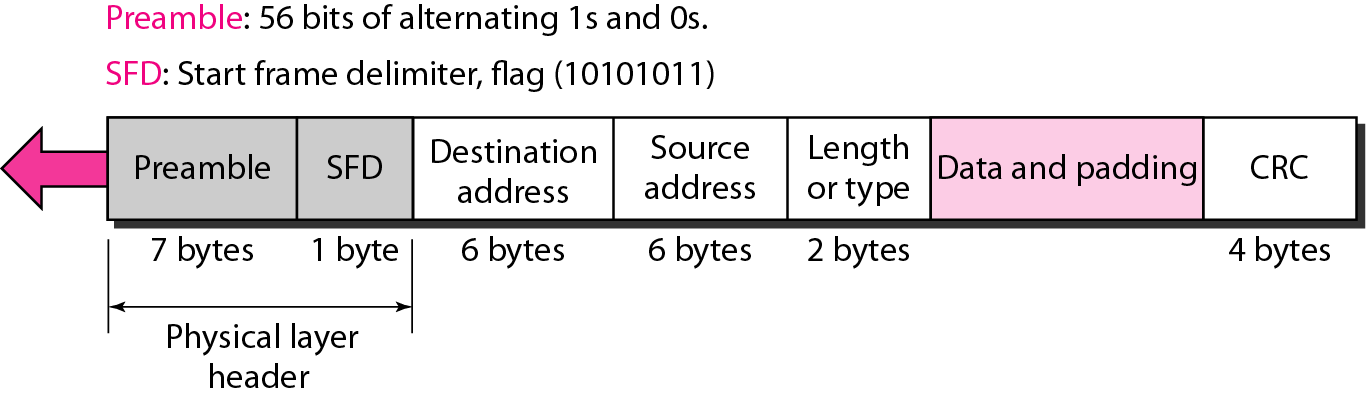
* In standard Ethernet, the MAC sublayer governs the operation of the access method.
* It also frames data received from the upper layers and passes them to the physical layer.

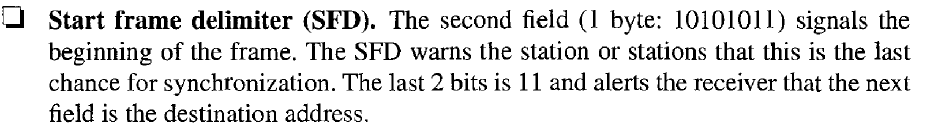
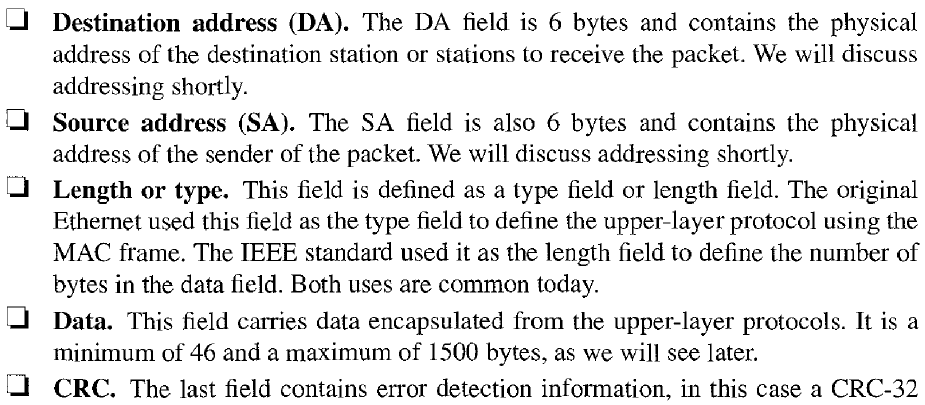
**Frame Format**

* Ethernet does not provide any mechanism for acknowledging received frames.
* This frame contains **7 fields**: **preamble, SFD, DA, SA, length or type of protocol data unit, upper-layer data and CRC**.

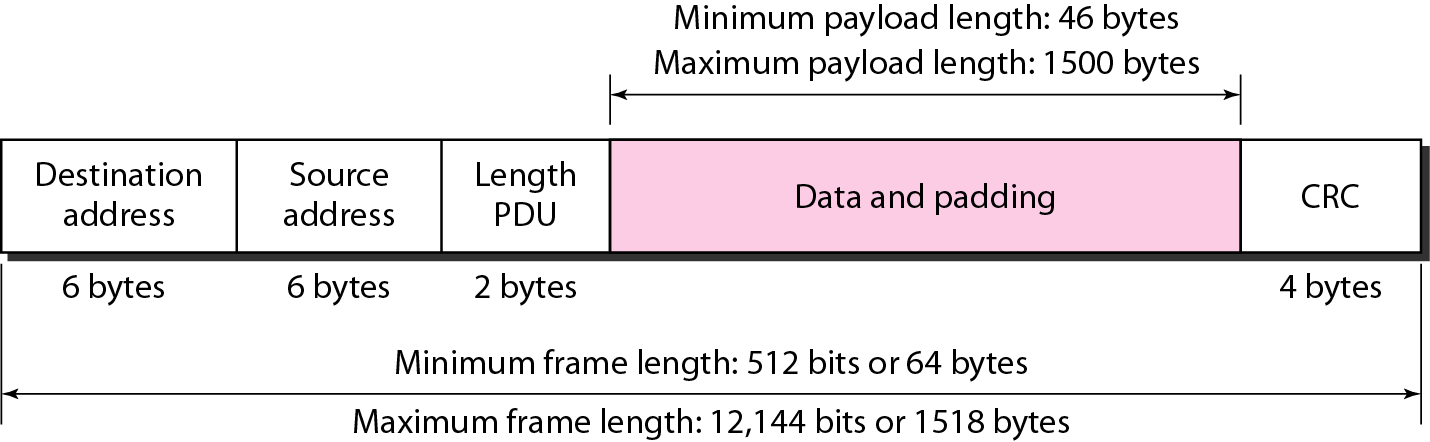


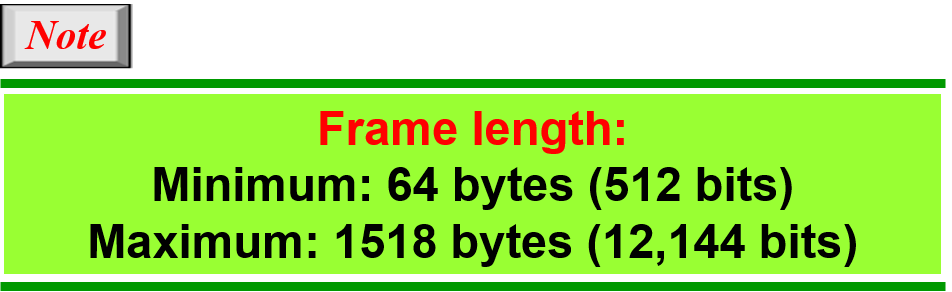
**Figure 13.4 *802.3 MAC frame***





**Figure *Minimum and maximum lengths***





**Addressing:**

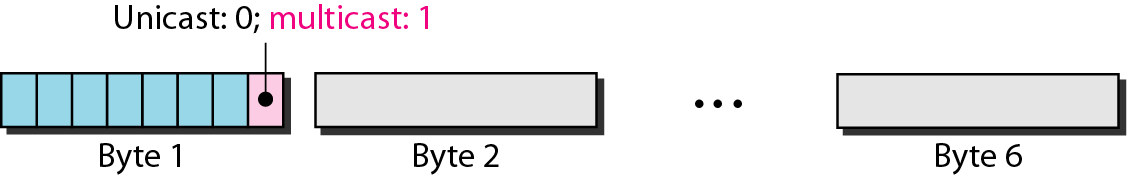
* Each station on an Ethernet network has its own Network Interface Card (NIC).
* The NIC fits inside the station and provides the station with a 6-byte physical address.
* The Ethernet address is a 6-byte (48 bits), normally written in hexa-decimal notation, with a colon between bytes.

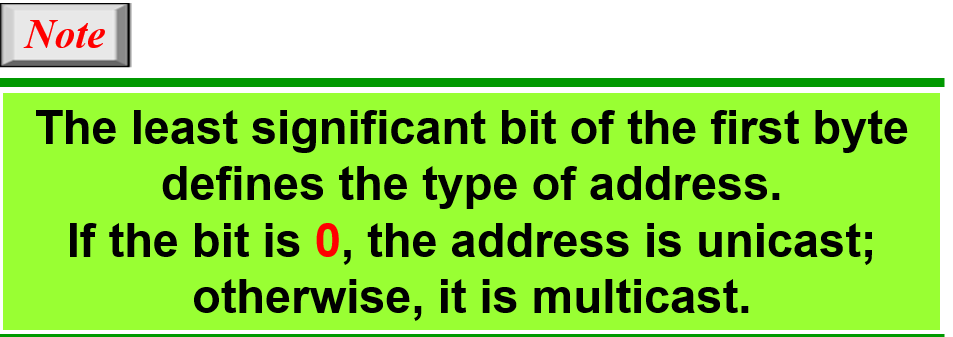


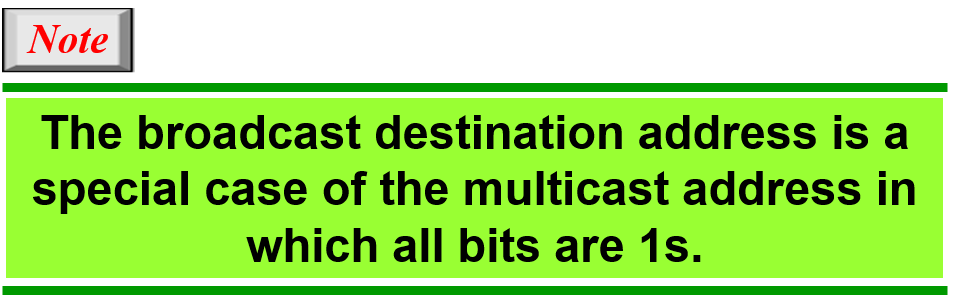
**Figure *Example of an Ethernet address in hexadecimal notation***

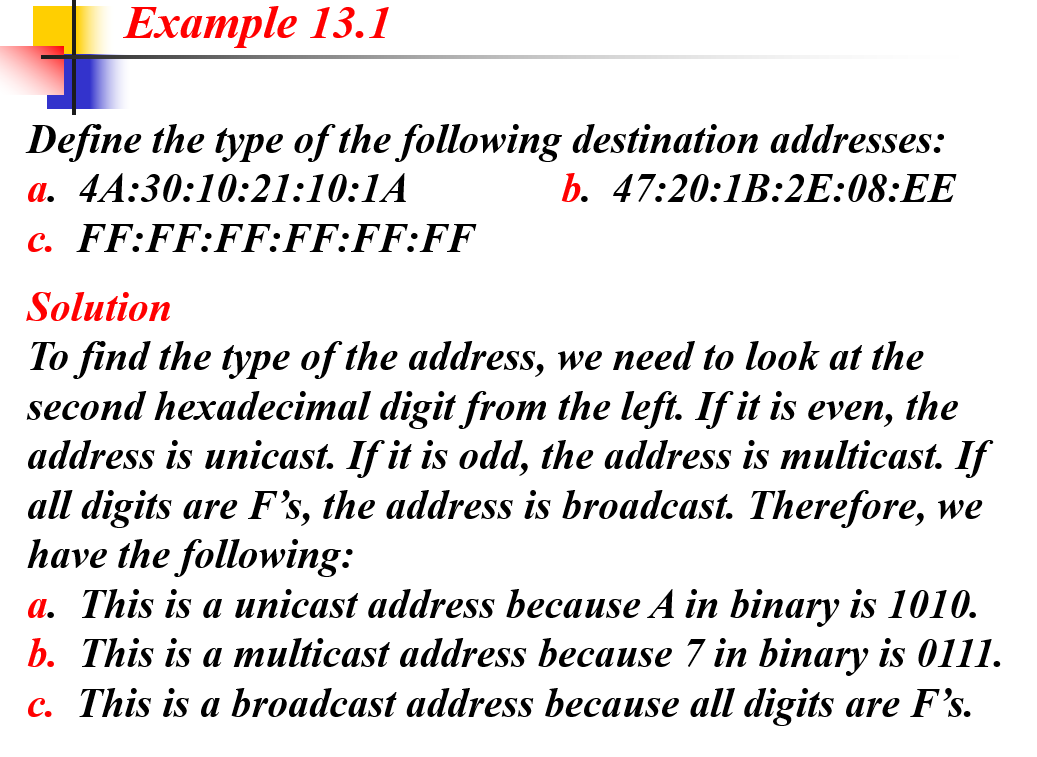
**Unicast, multicast and broadcast addresses:**

* A source address is always a unicast address- the frame comes from only one station.
* The destination address, however, can be unicast, multicast or broad cast address.
* If the least significant bit for the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.
* A unicast destination address defines only one recipient and the relationship between sender and receiver is one-to-one.
* A multicast destination address defines a group of addresses and the relationship between sender and receiver is one-to-many.
* The broadcast address is a special case of multicast address and the recipients are all the stations in the LAN.









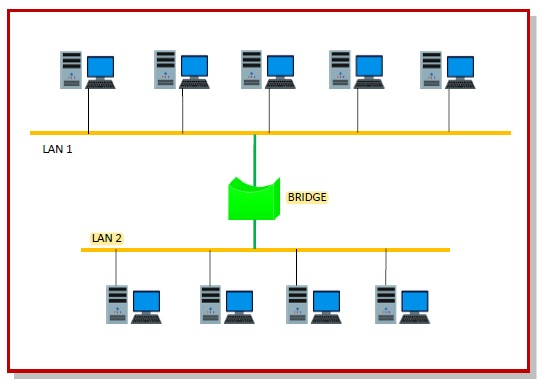
**Data Link Layer Switching:**

* Network switching is the process of forwarding data frames or packets from one port to another leading to data transmission from source to destination.
* Data link layer is the second layer of the Open System Interconnections (OSI) model whose function is to divide the stream of bits from physical layer into data frames and transmit the frames according to switching requirements.
* Switching in data link layer is done by network devices called **bridges**.

**Bridges:**

* A data link layer bridge connects multiple LANs (local area networks) together to form a larger LAN. This process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network.
* A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

The following diagram shows a bridge connecting two LANs −



**Switching by Bridges:**

When a data frame arrives at a particular port of a bridge, the bridge examines the frame’s data link address, or more specifically, the MAC address. If the destination addresses as well as the required switching is valid, the bridge sends the frame to the destined port. Otherwise, the frame is discarded.

The bridge is not responsible for end-to-end data transfer. It is concerned with transmitting the data frame from one hop to the next. Hence, they do not examine the payload field of the frame. Due to this, they can help in switching any kind of packets from the network layer above.

Bridges also connect virtual LANs (VLANs) to make a larger VLAN.

If any segment of the bridged network is wireless, a wireless bridge is used to perform the switching.

There are three main ways for bridging −

* simple bridging
* multi-port bridging
* learning or transparent bridging.

## Uses of Bridge:

* Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
* By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
* Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
  + If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
  + If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
* By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
* In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
* In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
* Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
* Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
* A wireless bridge is used to connect wireless networks or networks having a wireless segment.

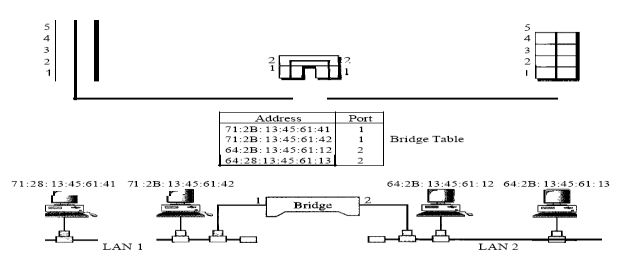
**learning bridges, spanning tree bridges**

Learning Bridges :

A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame. One may ask, What is the difference in functionality between a bridge and a repeater? A bridge has filtering capability. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port. A bridge has a table that maps addresses to ports.

Let us give an example. In Figure 1, two LANs are connected by a bridge. If a frame destined for station 712B13456142 arrives at port 1, the bridge consults its table to find the departing port. According to its table, frames for 7l2B13456142 leave through port 1; therefore, there is no need for forwarding, and the frame is dropped. On the other hand, if a frame for 712B13456141 arrives at port 2, the departing port is port 1 and the frame is forwarded. In the first case, LAN 2 remains free of traffic; in the second case, both LANs have traffic. In our example, we show a two-port bridge; in reality a bridge usually has more ports. Note also that a bridge does not change the physical addresses contained in the frame.

Figure 1 A bridge connecting two LANs



Transparent Bridges A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence. If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary. According to the IEEE 802.1 d specification, a system equipped with transparent bridges must meet three criteria:

I. Frames must be forwarded from one station to another.

2.The forwarding table is automatically made by learning frame movements in the network.

3. Loops in the system must be prevented.

Forwarding A transparent bridge must correctly forward the frames, as discussed in the previous section. Learning The earliest bridges had forwarding tables that were static. The systems administrator would manually enter each table entry during bridge setup. Although the process was simple, it was not practical. If a station was added or deleted, the table had to be modified manually. The same was true if a station's MAC address changed, which is not a rare event. For example, putting in a new network card means a new MAC address.

A better solution to the static table is a dynamic table that maps addresses to ports automatically. To make a table dynamic, we need a bridge that gradually learns from the frame movements. To do this, the bridge inspects both the destination and the source addresses. The destination address is used for the forwarding decision (table lookup); the source address is used for adding entries to the table and for updating purposes.

Let us elaborate on this process by using Figure 1.1 :

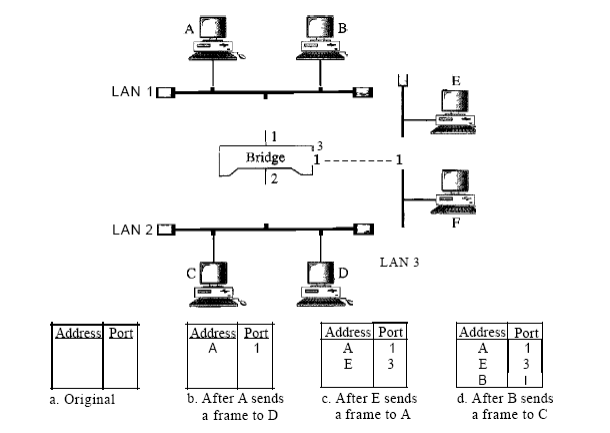


Figure 1.1 A learning bridge and the process of learning

1. When station A sends a frame to station D, the bridge does not have an entry for either D or A. The frame goes out from all three ports; the frame floods the network. However, by looking at the source address, the bridge learns that station A must be located on the LAN connected to port 1. This means that frames destined for A, in the future, must be sent out through port 1. The bridge adds this entry to its table. The table has its first entry now.

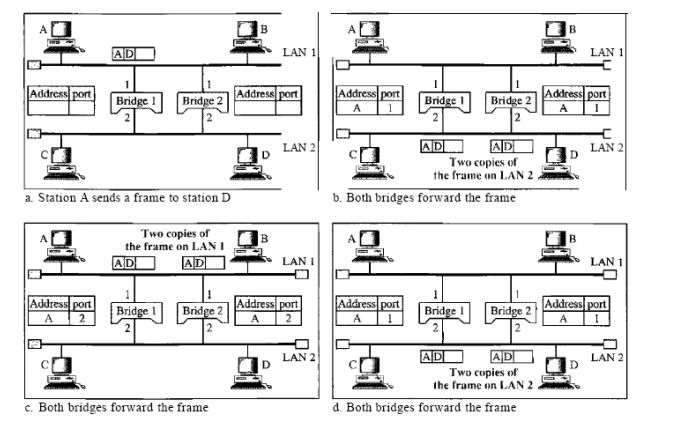
2. When station E sends a frame to station A, the bridge has an entry for A, so it forwards the frame only to port 1. There is no flooding. In addition, it uses the source address of the frame, E, to add a second entry to the table.

3. When station B sends a frame to C, the bridge has no entry for C, so once again it floods the network and adds one more entry to the table.

4. The process of learning continues as the bridge forwards frames.

Loop Problem Transparent bridges work fine as long as there are no redundant bridges in the system. Systems administrators, however, like to have redundant bridges (more than one bridge between a pair of LANs) to make the system more reliable. If a bridge fails, another bridge takes over until the failed one is repaired or replaced. Redundancy can create loops in the system, which is very undesirable. Figure 1.3 shows a very simple example of a loop created in a system with two LANs connected by two bridges.

Figure 1.3 Loop problem in a learning bridge



1. Station A sends a frame to station D. The tables of both bridges are empty. Both forward the frame and update their tables based on the source address A.

2. Now there are two copies of the frame on LAN 2. The copy sent out by bridge 1 is received by bridge 2, which does not have any information about the destination address D; it floods the bridge. The copy sent out by bridge 2 is received by bridge 1 and is sent out for lack of information about D. Note that each frame is handled separately because bridges, as two nodes on a network sharing the medium, use an access method such as CSMA/CD. The tables of both bridges are updated, but still there is no information for destination D.

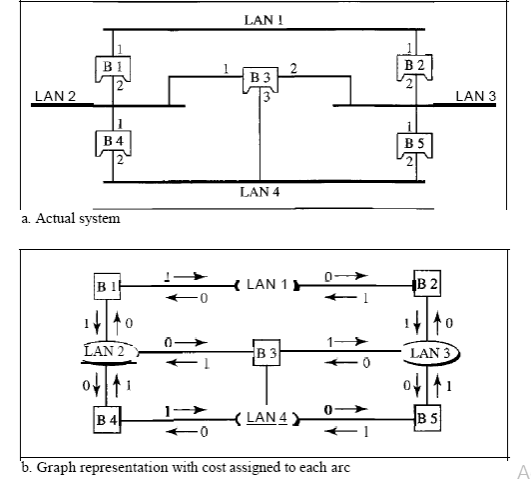
3. Now there are two copies of the frame on LAN 1. Step 2 is repeated, and both copies flood the network.

4. The process continues on and on. Note that bridges are also repeaters and regenerate frames. So in each iteration, there are newly generated fresh copies of the frames. To solve the looping problem, the IEEE specification requires that bridges use the spanning tree algorithm to create a loopless topology.

Spanning Tree :

In graph theory, a spanning tree is a graph in which there is no loop. In a bridged LAN, this means creating a topology in which each LAN can be reached from any other LAN through one path only (no loop). We cannot change the physical topology of the system because of physical connections between cables and bridges, but we can create a logical topology that overlays the physical one. Figure 1.4 shows a system with four LANs and five bridges. We have shown the physical system and its representation in graph theory. Although some textbooks represent the LANs as nodes and the bridges as the connecting arcs, we have shown both LANs and bridges as nodes. The connecting arcs show the connection of a LAN to a bridge and vice versa. To find the spanning tree, we need to assign a cost (metric) to each arc. The interpretation of the cost is left up to the systems administrator. It may be the path with minimum hops (nodes), the path with minimum delay, or the path with maximum bandwidth. If two ports have the same shortest value, the systems administrator just chooses one. We have chosen the minimum hops.

Figure 1.4 A system of connected LANs and its graph representation



The process to find the spanning tree involves three steps:

1. Every bridge has a built-in ID (normally the serial number, which is unique). Each bridge broadcasts this ID so that all bridges know which one has the smallest ID. The bridge with the smallest ID is selected as the root bridge (root of the tree). We assume that bridge B1 has the smallest ID. It is, therefore, selected as the root bridge.
2. The algorithm tries to find the shortest path (a path with the shortest cost) from the root bridge to every other bridge or LAN. The shortest path can be found by examining the total cost from the root bridge to the destination. Figure 1.5 shows the shortest paths.
3. The combination of the shortest paths creates the shortest tree.
4. Based on the spanning tree, we mark the ports that are part of the spanning tree, the forwarding ports, which forward a frame that the bridge receives. We also mark those ports that are not part of the spanning tree, the blocking ports, which block the frames received by the bridge. Figure 1.6 shows the physical systems of LANs with forwarding points (solid lines) and blocking ports (broken lines).

Figure 1.5 Finding the shortest paths and the spanning tree in a system of bridges

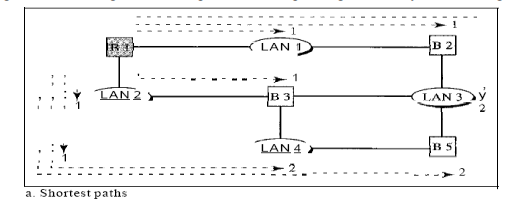
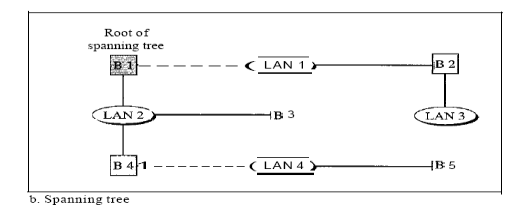


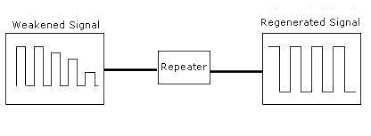
Figure 1.6 forwarding and blocking ports after using spanning tree algorithm



REPEATERS, HUBS, BRIDGES, SWITCHES

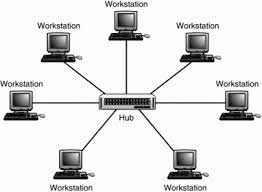
**REPEATERS:**

 A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.



**HUBS**

 A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches. Hubs cannot filter data, so data packets are sent to all connected devices. They do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.



There are different types of hubs

**Types of Hub**

* **Active Hub:-**These are the hubs that have their own power supply. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
* **Passive Hub :-**These are the hubs that collect wiring from nodes and power supply from the active hub. They cannot be used to extend the distance between nodes.
* **Intelligent Hub :-**It works like active hubs and includes remote management capabilities. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

**BRIDGES**

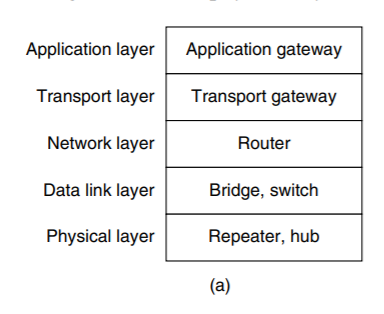
A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.



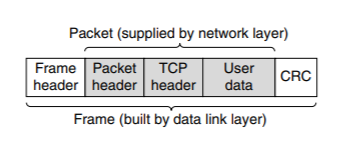
**Switches**

A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

All these devices operate in different layers as illustrated in below figure. The layer matters because different devices use different pieces of information to decide how to switch.



A header is added in every layer shown as follows:



**Repeaters:**

* The repeater operates in the physical layer.
* These are analog devices that work with signals on the cables to which they are connected.
* A signal appearing on one cable is regenerated and put out on another cable. Hence it extends the physical length of LAN.
* Repeaters do not understand frames, packets or headers. They understand the symbols that encode bit as volts.
* Classic Ethernet, for example, was designed to allow four repeaters that would boost the signal to extend the maximum cable length from 500 meters to 2500 meters.

**Hub:**

* A hub has a number of input lines that it joins electrically. Active hub and passive hub are two types of hubs.
* Frames arriving on any of the lines are sent out on all the others. It is broadcast device. If two frames arrive at the same time, they will collide, just as on a coaxial cable.
* All the lines coming into a hub must operate at the same speed. Hubs differ from repeaters in that they do not boost the incoming signals and are designed for multiple input lines, but the differences are slight.
* Like repeaters, hubs are physical layer devices that do not examine the link layer addresses or use them in any way. It is not an intelligent device.

**Bridge**:

* A bridge connects two or more LANs. It operates at data link layer.
* Like a hub, a modern bridge has multiple ports, usually enough for 4 to 48 input lines of a certain type. Unlike in a hub, each port is isolated to be its own collision domain.
* When a frame arrives, the bridge extracts the destination address (for Ethernet, it is 48 bit) from the frame header and looks it up in a table to see where to send the frame.
* The bridge only outputs the frame on the port where it is needed and can forward multiple frames at the same time.
* Filtering, forwarding and blocking of frames are functions of bridges.
* Bridges offer much better performance than hubs and the isolation between bridge ports also means that the input lines may run at different speeds, possibly even with different network types. A common example is a bridge with ports that connect to 10-, 100-, and 1000-Mbps Ethernet.
* Buffering within the bridge is needed to accept a frame on one port and transmit the frame out on a different port.
* Bridges were originally intended to be able to join different kinds of LANs, for example, an Ethernet and a Token Ring LAN. However, this never worked well because of differences between the LANs such as frame formats, maximum frame lengths, security and Quality of service.

**Switch:**

* Switches are modern bridges by another name. It acts as multiport bridge to connect devices or segments in a LAN. It operates at data link layer.
* It is point to point device.
* It is an intelligent device. It uses switching table to find the correct destination.
* Switches are of two types:

i. Store-and-forward switch: It stores the frame in the input buffer until the whole packet has arrived.

ii. Cut-through switch: It forwards the packet to the output buffer as soon as the destination address is received.

* Also there are layer 2 (bridge) and layer 3 switches (kind of router). It is sophisticated and expensive device.

**PERIODIC & APERIODIC SIGNALS**

Data transmitted over the network can be Analog or Digital. Both Analog and Digital signals can take one of two forms:

* Periodic
* Non-Periodic (Aperiodic)

A **periodic** signal is a signal that repeats the sequence of values exactly after a fixed length of time, known as the period. It completes the pattern within a measurable time frame. The completion of one full pattern is called a cycle.

**Ex:** When a flight is detected by the radar and until the radar exists, the radar signal zone is an example of a periodic real-time task.

A **Non-periodic (Aperiodic)** changes without any pattern or cycle that repeats over time.

**Ex:** Typing on the Keyboard.

Both analog and digital signals can be periodic and aperiodic. But in data communications, **periodic analog signals** and **aperiodic digital signals** are commonly used.

**Periodic Analog Signals:**

Periodic Analog Signals can be of two types:

* **Simple** : A simple periodic analog signal is a Sine wave
* **Composite:**  A composite periodic analog signal is composed of multiple sine waves.

**Sine Wave:**

The sine wave is the most fundamental form of a periodic signal, represented in Fig.1.

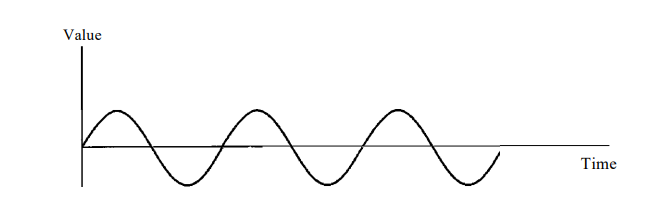


Fig.1. Sine Wave

To describe and understand the sine wave completely, it can be done using three parameters. they are:

* Peak amplitude
* Frequency
* Phase

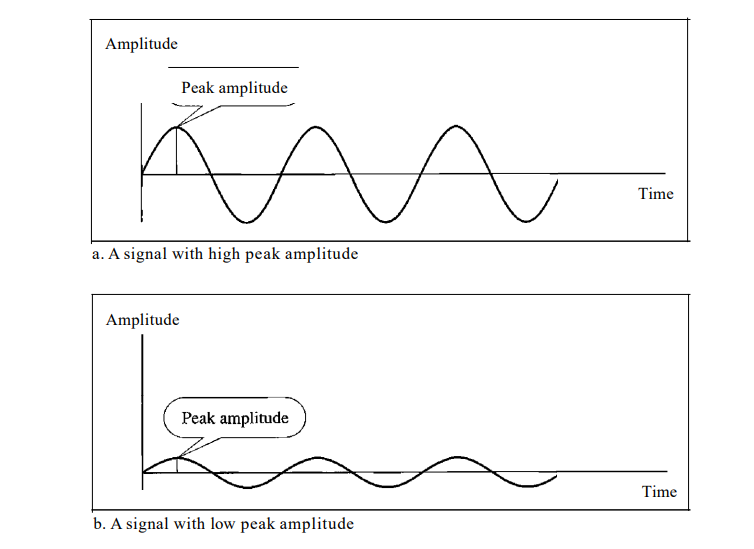
**Peak Amplitude:**  The peak amplitude of a signal is the value of its highest intensity. It is measured in volts.

Fig.2. Two different signals with different Peak Amplitudes

**Ex:** The power in the house can be represented by sine wave with a peak amplitude of 155 to 170 volts.

**Period and Frequency:** Period refere to the amount of time needed for a signal to complete one cycle. It is measured in seconds.

Frequency is the number of periods in one second. It is measured or expressed in Hertz (Hz). Period is the inverse of frequency and frequency is the inverse of the period. The formulae is given as follows:

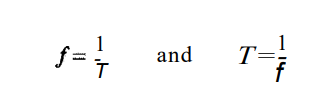


Fig.3. Formulae for Frequency and Period.

**xample:**

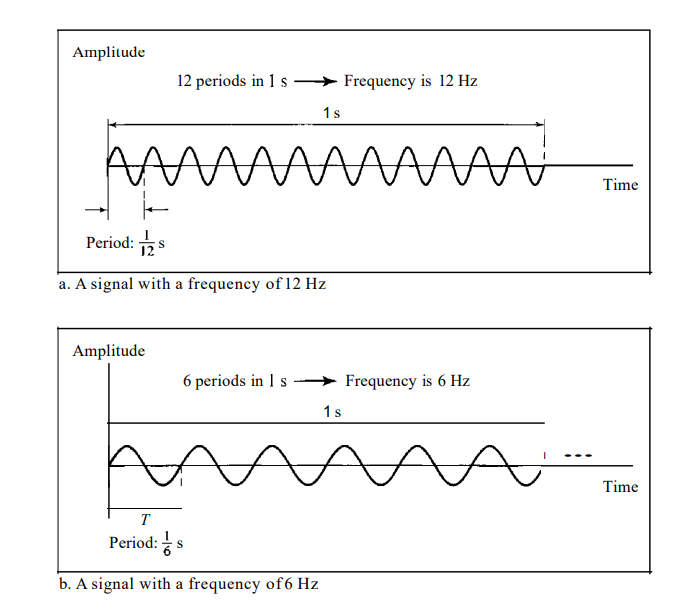


Fig.4. Example

**Phase:**  The term Phase describes the position of waveform relative to time 0. It is measured in radians.

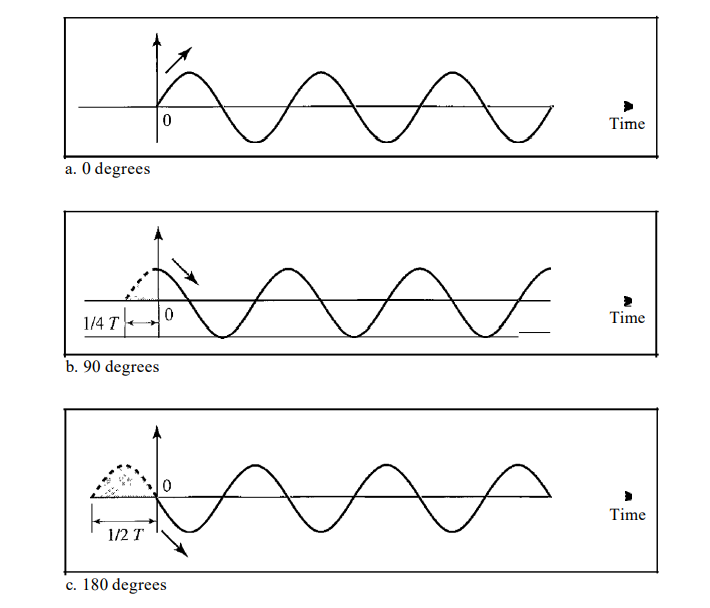


Fig.5. Three sine waves with different Phases.

From Fig.5.

* A sine wave with a phase of 0° starts at time 0 with a zero amplitude. The amplitude is increasing.
* A sine wave with a phase of 90° starts at time 0 with a peak amplitude. The amplitude is decreasing.
* A sine wave with a phase of 180° starts at time 0 with a zero amplitude. The amplitude is decreasing.

Another way to look at the phase is in terms of shift or offset. We can say that

* A sine wave with a phase of 0° is not shifted.
* A sine wave with a phase of 90° is shifted to the left by ¼ cycle.
* A sine wave with a phase of 180° is shifted to the left by ½ cycle.

**Encoding** is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of data. **Decoding** is the reverse process of encoding which is to extract the information from the converted format.

Data Encoding

Encoding is the process of using various patterns of voltage or current levels to represent **1s** and **0s** of the digital signals on the transmission link.

The common types of line encoding are Unipolar, Polar, Bipolar, and Manchester.

Encoding Techniques

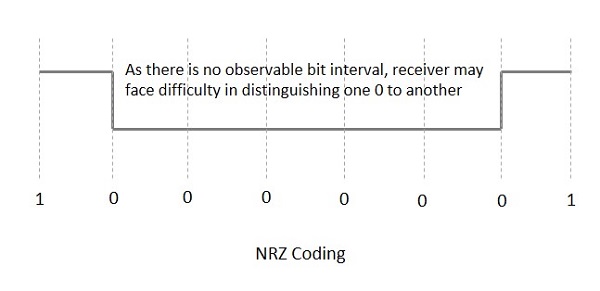
The data encoding technique is divided into the following types, depending upon the type of data conversion.

* **Analog data to Analog signals** − The modulation techniques such as Amplitude Modulation, Frequency Modulation and Phase Modulation of analog signals, fall under this category.
* **Analog data to Digital signals** − This process can be termed as digitization, which is done by Pulse Code Modulation PCMPCM. Hence, it is nothing but digital modulation. As we have already discussed, sampling and quantization are the important factors in this. Delta Modulation gives a better output than PCM.
* **Digital data to Analog signals** − The modulation techniques such as Amplitude Shift Keying ASKASK, Frequency Shift Keying FSKFSK, Phase Shift Keying PSKPSK, etc., fall under this category. These will be discussed in subsequent chapters.
* **Digital data to Digital signals** − These are in this section. There are several ways to map digital data to digital signals. Some of them are −

**Non Return to Zero NRZNRZ**

NRZ Codes has **1** for High voltage level and **0** for Low voltage level. The main behavior of NRZ codes is that the voltage level remains constant during bit interval. The end or start of a bit will not be indicated and it will maintain the same voltage state, if the value of the previous bit and the value of the present bit are same.

The following figure explains the concept of NRZ coding.



If the above example is considered, as there is a long sequence of constant voltage level and the clock synchronization may be lost due to the absence of bit interval, it becomes difficult for the receiver to differentiate between 0 and 1.

There are two variations in NRZ namely −

**NRZ - L NRZ–LEVELNRZ–LEVEL**

There is a change in the polarity of the signal, only when the incoming signal changes from 1 to 0 or from 0 to 1. It is the same as NRZ, however, the first bit of the input signal should have a change of polarity.

**NRZ - I NRZ–INVERTEDNRZ–INVERTED**

If a **1** occurs at the incoming signal, then there occurs a transition at the beginning of the bit interval. For a **0** at the incoming signal, there is no transition at the beginning of the bit interval.

NRZ codes has a **disadvantage** that the synchronization of the transmitter clock with the receiver clock gets completely disturbed, when there is a string of **1s** and **0s**. Hence, a separate clock line needs to be provided.

**Bi-phase Encoding**

The signal level is checked twice for every bit time, both initially and in the middle. Hence, the clock rate is double the data transfer rate and thus the modulation rate is also doubled. The clock is taken from the signal itself. The bandwidth required for this coding is greater.

There are two types of Bi-phase Encoding.

* Bi-phase Manchester
* Differential Manchester

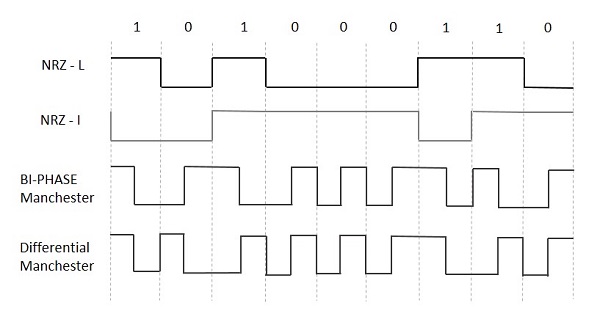
**Bi-phase Manchester**

In this type of coding, the transition is done at the middle of the bit-interval. The transition for the resultant pulse is from High to Low in the middle of the interval, for the input bit 1. While the transition is from Low to High for the input bit **0**.

**Differential Manchester**

In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is **0**. If no transition occurs at the beginning of the bit interval, then the input bit is **1**.

The following figure illustrates the waveforms of NRZ-L, NRZ-I, Bi-phase Manchester and Differential Manchester coding for different digital inputs.



**Block Coding**

Among the types of block coding, the famous ones are 4B/5B encoding and 8B/6T encoding. The number of bits are processed in different manners, in both of these processes.

**4B/5B Encoding**

In Manchester encoding, to send the data, the clocks with double speed is required rather than NRZ coding. Here, as the name implies, 4 bits of code is mapped with 5 bits, with a minimum number of **1** bits in the group.

The clock synchronization problem in NRZ-I encoding is avoided by assigning an equivalent word of 5 bits in the place of each block of 4 consecutive bits. These 5-bit words are predetermined in a dictionary.

The basic idea of selecting a 5-bit code is that, it should have **one leading 0** and it should have **no more than two trailing 0s**. Hence, these words are chosen such that two transactions take place per block of bits.

**8B/6T Encoding**

We have used two voltage levels to send a single bit over a single signal. But if we use more than 3 voltage levels, we can send more bits per signal.

For example, if 6 voltage levels are used to represent 8 bits on a single signal, then such encoding is termed as 8B/6T encoding. Hence in this method, we have as many as 729 3636 combinations for signal and 256 2828 combinations for bits.

These are the techniques mostly used for converting digital data into digital signals by compressing or coding them for reliable transmission of data.

**RS-232C PROTOCOL**

**DATA LINK LAYER DESIGN ISSUES**

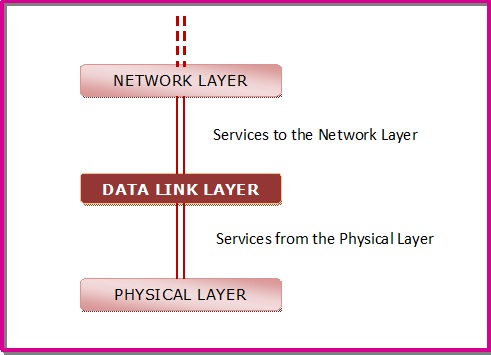
The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

* Providing services to the network layer
* Framing
* Error Control
* Flow Control

**Services to the Network Layer**

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer.The primary function of this layer is to provide a well defined service interface to network layer above it.



The types of services provided can be of three types −

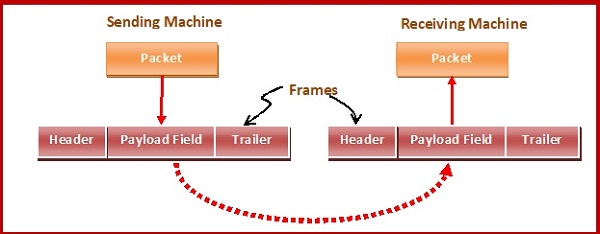
* Unacknowledged connectionless service
* Acknowledged connectionless service
* Acknowledged connection - oriented service

**Framing**

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

* Frame Header
* Payload field that contains the data packet from network layer
* Trailer



**Error Control**

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

* Dealing with transmission errors
* Sending acknowledgement frames in reliable connections
* Retransmitting lost frames
* Identifying duplicate frames and deleting them
* Controlling access to shared channels in case of broadcasting

**Flow Control**

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

* Feedback based flow control
* Rate based flow control

**Routers and Gateways**

**What is a router?**

A router is a switching device for networks, which is able to route network packets, based on their addresses, to other networks or devices. Among other things, they are used for Internet access, for coupling networks or for connecting branch offices to a central office via VPN (Virtual Private Network). Depending on the type they communicate using the various access protocols, such as Ethernet, ATM or DSL. In the OSI layer model, the switching of data packets through the router is based on the address on the network layer (layer 3). In addition to routers that use Internet protocol (IP), there are multi-protocol routers, which also handle other network protocols.

**How a router functions?**

A router has multiple interfaces and receives data packets through them. It evaluates the network addresses of the incoming packets and decides which interface to forward the packet to. It uses its local routing table for decision-making. This can be statically configured or calculated via dynamic routing protocols such as OSPF or BGP.

**The various types of routers**

Routers are optimised to suit a particular purpose, depending on their application. So-called backbone routers are high-performance routers of the carrier class, which route and forward packets with rapid speeds of several gigabits per second. They are housed in data centres, and may be as large as several 19-inch cabinets.  
  
For interfacing with networks of other providers, Internet service providers may use border routers or edge routers, which mainly use the routing protocol BGP. This routing protocol allows for the optimum the exchange of routes. Most of these routers also support the prioritisation of traffic via Quality of Service.  
  
For connecting to the Internet, access routers are used, which allow devices in a local area network to access Internet via DSL, cable, wireless or ISDN.

**Routers and telephony**

Many Internet routers have additional functions for telephony. They often have full [telephone systems](https://www.nfon.com/en/telephony/cloudya) integrated within the devices. Analogue or digital telephones may be connected to them, as well as cordless DECT phones or Voice-over-IP phones, depending on the type. While a normal Internet connection provides sufficient access for VoIP telephony, routers with telephone systems for standard telephony need interfaces for access to the analogue or digital (ISDN) telephone network.

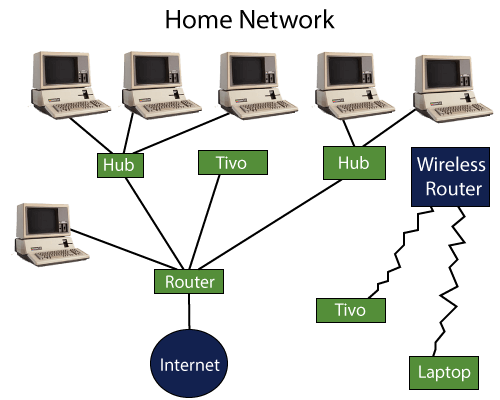
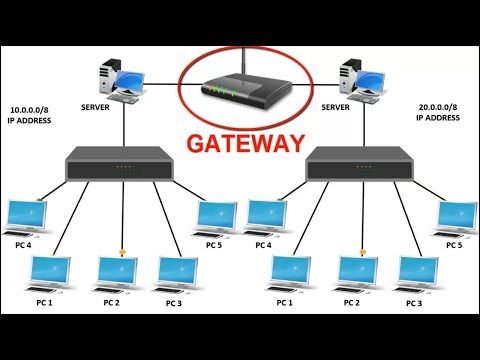


Fig: A Router

### Gateways

A gateway is a [network node](https://www.techtarget.com/searchnetworking/definition/node) used in telecommunications that connects two networks with different transmission [protocols](https://www.techtarget.com/searchnetworking/definition/protocol) together. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed. In most [IP](https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol)-based networks, the only traffic that does not go through at least one gateway is traffic flowing among nodes on the same local area network ([LAN](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN)) segment. The term default gateway or network gateway may also be used to describe the same concept.

The primary advantage of using a gateway in personal or enterprise scenarios is simplifying internet connectivity into one device. In the enterprise, a gateway node can also act as a [proxy server](https://whatis.techtarget.com/definition/proxy-server) and a [firewall](https://www.techtarget.com/searchsecurity/definition/firewall). Gateways can be purchased through popular technology retailers, such as Best Buy, or rented through an internet service provider.



### Fig: Gateway

### How gateways work?

All networks have a boundary that limits communication to devices that are directly connected to it. Due to this, if a network wants to communicate with devices, nodes or networks outside of that boundary, they require the functionality of a gateway. A gateway is often characterized as being the combination of a [router](https://www.techtarget.com/searchnetworking/definition/router) and a [modem](https://searchmobilecomputing.techtarget.com/definition/modem).

The gateway is implemented at the edge of a network and manages all data that is directed internally or externally from that network. When one network wants to communicate with another, the data packet is passed to the gateway and then routed to the destination through the most efficient path. In addition to routing data, a gateway will also store information about the host network’s internal paths and the paths of any additional networks that are encountered.

Gateways are basically protocol converters, facilitating compatibility between two protocols and operating on any layer of the open systems interconnection ([OSI](https://www.techtarget.com/searchnetworking/definition/OSI)) model.

### Types of gateways

Gateways can take several forms and perform a variety of tasks. Examples of this include:

* [Web application firewalls](https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF)- This type filters traffic to and from a web server and looks at application-layer data.
* [Cloud storage gateways](https://www.techtarget.com/searchstorage/definition/cloud-storage-gateway)- This type translates storage requests with various cloud storage service API calls. It allows organizations to integrate storage from a private cloud into applications without migrating into a public cloud.
* [API](https://searchapparchitecture.techtarget.com/definition/application-program-interface-API), [SOA](https://searchapparchitecture.techtarget.com/definition/service-oriented-architecture-SOA) or XML gateways – This type manages traffic flowing into and out of a service, microservices-oriented architecture or XML-based web service.
* [IoT gateways](https://whatis.techtarget.com/definition/IoT-gateway)-This type aggregates sensor data from devices in an IoT environment, translates between sensor protocols and processes sensor data before sending it onward.
* [Media gateways](https://www.techtarget.com/searchunifiedcommunications/definition/media-gateway)- This type converts data from the format required for one type of network to the format required for another.
* Email security gateways- This type prevents the transmission of emails that break company policy or will transfer information with malicious intent.
* [VoIP trunk gateways](https://www.techtarget.com/searchunifiedcommunications/definition/VoIP-trunk-gateway)- This type facilitates the use of plain old telephone service equipment, such as landline phones and fax machines, with a voice over IP (VoIP) network.

Additionally, a service provider may develop their own personal gateways that can be used by customers. For instance, Amazon Web Services (AWS) has an [Amazon API Gateway](https://searchaws.techtarget.com/definition/Amazon-API-Gateway) that allows a developer to connect non-AWS applications to AWS back end resources.

### Difference between a gateway and a router

Gateways and routers are similar in that they both can be used to regulate traffic between two or more separate networks. However, a router is used to join two similar types of networks and a gateway is used to join two dissimilar networks. Dissimilar could be used to describe networks that use different primary protocols.

Due to this logic, a router may be considered a gateway, but a gateway is not always considered a router. Routers are the most common gateway, used to connect a home or enterprise network to the internet

**Bluetooth**

In 1994, the L. M. Ericsson company became interested in connecting its mobile phones to other devices (e.g., PDAs) without cables. Together with four other companies (IBM, Intel, Nokia, and Toshiba), it formed a SIG (Special Interest Group, i.e., consortium) to develop a wireless standard for interconnecting computing and communication devices and accessories using short-range, low-power, inexpensive wireless radios. The project was named **Bluetooth**, after Harald Blaatand (Bluetooth) II (940-981), a Viking king who unified (i.e., conquered) Denmark and Norway, also without cables.

**Bluetooth Architecture**

The basic unit of a Bluetooth system is a **piconet**, which consists of a master node and up to seven active slave nodes within a distance of 10 meters. Multiple piconets can exist in the same (large) room and can even be connected via a bridge node, as shown in Fig. 4-35. An interconnected collection of piconets is called a **scatternet**

***Figure 4-35. Two piconets can be connected to form a scatternet***



**Bluetooth Applications**

Most network protocols just provide channels between communicating entities and let applications designers figure out what they want to use them for. For example, 802.11 does not specify whether users should use their notebook computers for reading e-mail, surfing the Web, or something else. In contrast, the Bluetooth V1.1 specification names 13 specific applications to be supported and provides different protocol stacks for each one. Unfortunately, this approach leads to a very large amount of complexity, which we will omit here. The 13 applications, which are called **profiles**, are listed in Fig. 4-36. By looking at them briefly now, we may see more clearly what the Bluetooth SIG is trying to accomplish.

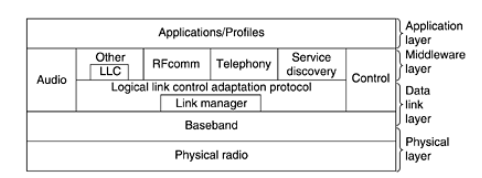
***The Bluetooth profiles.***



**The Bluetooth Protocol Stack**

The Bluetooth standard has many protocols grouped loosely into layers. The layer structure does not follow the OSI model, the TCP/IP model, the 802 model, or any other known model. However, IEEE is working on modifying Bluetooth to shoehorn it into the 802 model better. The basic Bluetooth protocol architecture as modified by the 802 committee is shown in Fig. 4- 37.

***Figure 4-37. The 802.15 version of the Bluetooth protocol architecture.***

******

The bottom layer is the physical radio layer, which corresponds fairly well to the physical layer in the OSI and 802 models. It deals with radio transmission and modulation. Many of the concerns here have to do with the goal of making the system inexpensive so that it can become a mass market item. The baseband layer is somewhat analogous to the MAC sublayer but also includes elements of the physical layer. It deals with how the master controls time slots and how these slots are grouped into frames. Next comes a layer with a group of somewhat related protocols. The link manager handles the establishment of logical channels between devices, including power management, authentication, and quality of service. The logical link control adaptation protocol (often called L2CAP) shields the upper layers from the details of transmission. It is analogous to the standard 802 LLC sublayer, but technically different from it. As the names suggest, the audio and control protocols deal with audio and control, respectively. The applications can get at them directly, without having to go through the L2CAP protocol. The next layer up is the middleware layer, which contains a mix of different protocols. The 802 LLC was inserted here by IEEE for compatibility with its other 802 networks. The RFcomm, telephony, and service discovery protocols are native. RFcomm (Radio Frequency communication) is the protocol that emulates the standard serial port found on PCs for connecting the keyboard, mouse, and modem, among other devices. It has been designed to allow legacy devices to use it easily. The telephony protocol is a real-time protocol used for the three speech-oriented profiles. It also manages call setup and termination. Finally, the service discovery protocol is used to locate services within the network. The top layer is where the applications and profiles are located. They make use of the protocols in lower layers to get their work done. Each application has its own dedicated subset of the protocols. Specific devices, such as a headset, usually contain only those protocols needed by that application and no others.

In the following sections we will examine the three lowest layers of the Bluetooth protocol stack since these roughly correspond to the physical and MAC sublayers.

**The Bluetooth Radio Layer**

The radio layer moves the bits from master to slave, or vice versa. It is a low-power system with a range of 10 meters operating in the 2.4-GHz ISM band. The band is divided into 79 channels of 1 MHz each. Modulation is frequency shift keying, with 1 bit per Hz giving a gross data rate of 1 Mbps, but much of this spectrum is consumed by overhead. To allocate the channels fairly, frequency hopping spread spectrum is used with 1600 hops/sec and a dwell time of 625 µsec. All the nodes in a piconet hop simultaneously, with the master dictating the hop sequence. Because both 802.11 and Bluetooth operate in the 2.4-GHz ISM band on the same 79 channels, they interfere with each other. Since Bluetooth hops far faster than 802.11, it is far more likely that a Bluetooth device will ruin 802.11 transmissions than the other way around. Since 802.11 and 802.15 are both IEEE standards, IEEE is looking for a solution to this problem, but it is not so easy to find since both systems use the ISM band for the same reason: no license is required there. The 802.11a standard uses the other (5 GHz) ISM band, but it has a much shorter range than 802.11b (due to the physics of radio waves), so using 802.11a is not a perfect solution for all cases. Some companies have solved the problem by banning Bluetooth altogether. A market-based solution is for the network with more power (politically and economically, not electrically) to demand that the weaker party modify its standard to stop interfering with it. Some thoughts on this matter are given in (Lansford et al., 2001).

The Bluetooth Baseband Layer

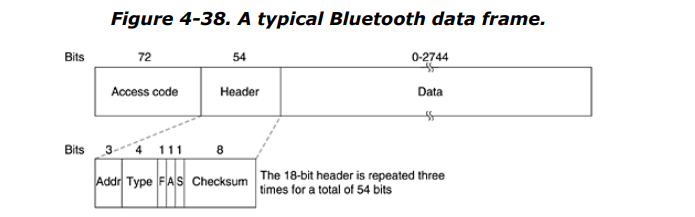
The baseband layer is the closest thing Bluetooth has to a MAC sublayer. It turns the raw bit stream into frames and defines some key formats. In the simplest form, the master in each piconet defines a series of 625 µsec time slots, with the master's transmissions starting in the even slots and the slaves' transmissions starting in the odd ones. This is traditional time division multiplexing, with the master getting half the slots and the slaves sharing the other half. Frames can be 1, 3, or 5 slots long. The frequency hopping timing allows a settling time of 250–260 µsec per hop to allow the radio circuits to become stable. Faster settling is possible, but only at higher cost. For a singleslot frame, after settling, 366 of the 625 bits are left over. Of these, 126 are for an access code and the header, leaving 240 bits for data. When five slots are strung together, only one settling period is needed and a slightly shorter settling period is used, so of the 5 x 625 = 3125 bits in five time slots, 2781 are available to the baseband layer. Thus, longer frames are much more efficient than single-slot frames. Each frame is transmitted over a logical channel, called a link, between the master and a slave. Two kinds of links exist. The first is the ACL (Asynchronous Connection-Less) link, which is used for packet-switched data available at irregular intervals. These data come from the L2CAP layer on the sending side and are delivered to the L2CAP layer on the receiving side. ACL traffic is delivered on a best-efforts basis. No guarantees are given. Frames can be lost and may have to be retransmitted. A slave may have only one ACL link to its master. The other is the SCO (Synchronous Connection Oriented) link, for real-time data, such as telephone connections. This type of channel is allocated a fixed slot in each direction. Due to the time-critical nature of SCO links, frames sent over them are never retransmitted. Instead, forward error correction can be used to provide high reliability. A slave may have up to three SCO links with its master. Each SCO link can transmit one 64,000 bps PCM audio channel.

**The Bluetooth L2CAP Layer**

The L2CAP layer has three major functions. First, it accepts packets of up to 64 KB from the upper layers and breaks them into frames for transmission. At the far end, the frames are reassembled into packets again. Second, it handles the multiplexing and demultiplexing of multiple packet sources. When a packet has been reassembled, the L2CAP layer determines which upper-layer protocol to hand it to, for example, RFcomm or telephony. Third, L2CAP handles the quality of service requirements, both when links are established and during normal operation. Also negotiated at setup time is the maximum payload size allowed, to prevent a large-packet device from drowning a small-packet device. This feature is needed because not all devices can handle the 64-KB maximum packet.

**The Bluetooth Frame Structure**

There are several frame formats, the most important of which is shown in Fig. 4-38. It begins with an access code that usually identifies the master so that slaves within radio range of two masters can tell which traffic is for them. Next comes a 54-bit header containing typical MAC sublayer fields. Then comes the data field, of up to 2744 bits (for a five-slot transmission). For a single time slot, the format is the same except that the data field is 240 bits.

****

Let us take a quick look at the header. The Address field identifies which of the eight active devices the frame is intended for. The Type field identifies the frame type (ACL, SCO, poll, or null), the type of error correction used in the data field, and how many slots long the frame is. The Flow bit is asserted by a slave when its buffer is full and cannot receive any more data. This is a primitive form of flow control. The Acknowledgement bit is used to piggyback an ACK onto a frame. The Sequence bit is used to number the frames to detect retransmissions. The protocol is stop-and-wait, so 1 bit is enough. Then comes the 8-bit header Checksum. The entire 18-bit header is repeated three times to form the 54-bit header shown in Fig. 4-38. On the receiving side, a simple circuit examines all three copies of each bit. If all three are the same, the bit is accepted. If not, the majority opinion wins. Thus, 54 bits of transmission capacity are used to send 10 bits of header. The reason is that to reliably send data in a noisy environment using cheap, low-powered (2.5 mW) devices with little computing capacity, a great deal of redundancy is needed. Various formats are used for the data field for ACL frames. The SCO frames are simpler though: the data field is always 240 bits. Three variants are defined, permitting 80, 160, or 240 bits of actual payload, with the rest being used for error correction. In the most reliable version (80-bit payload), the contents are just repeated three times, the same as the header. Since the slave may use only the odd slots, it gets 800 slots/sec, just as the master does. With an 80-bit payload, the channel capacity from the slave is 64,000 bps and the channel capacity

from the master is also 64,000 bps, exactly enough for a single full-duplex PCM voice channel (which is why a hop rate of 1600 hops/sec was chosen). These numbers mean that a fullduplex voice channel with 64,000 bps in each direction using the most reliable format completely saturates the piconet despite a raw bandwidth of 1 Mbps. For the least reliable variant (240 bits/slot with no redundancy at this level), three full-duplex voice channels can be supported at once, which is why a maximum of three SCO links is permitted per slave. There is much more to be said about Bluetooth, but no more space to say it here. For more information, see (Bhagwat, 2001; Bisdikian, 2001; Bray and Sturman, 2002; Haartsen, 2000; Johansson et al., 2001; Miller and Bisdikian, 2001; and Sairam et al., 2002).

**Wi-Fi**

We all know about **Wi-Fi**, in our mobile, laptop everywhere Wi-Fi is supported. Wi-Fi is a wireless networking technology, by which we can access networks or connect with other computers or mobile using a wireless medium. In Wi-Fi, data are transferred over radio frequencies in a circular range.

**Wi-Fi**,a brand name given by the Wi-Fi Alliance (formerly Wireless Ethernet Compatibility Alliance), is a generic term that refers to the communication standard for the wireless network which works as a Local Area Network to operate without using the cable and any types of wiring. It is known as **WLAN**. The communication standard is **IEEE 802.11**. Wi-Fi works using Physical Data Link Layer.

Nowadays in all mobile computing devices such as laptops, mobile phones, also digital cameras, smart TVs has the support of Wi-Fi. The Wi-Fi connection is established from the access point or base station to the client connection or any client-to-client connection within a specific range, the range depends on the router which provides the radio frequency through Wi-Fi. These frequencies operate on 2 types of bandwidth at present, 2.4 GHz and 5 GHz.

All the modern laptops and mobiles are capable of using both bandwidths, it depends on the Wi-Fi adapter which is inside the device to catch the Wi-Fi signal. 2.4 GHz is the default bandwidth supported by all the devices. 2.4 GHz can cover a big range of areas to spread the Wi-Fi signal but the frequency is low, so in simple words, the speed of the internet is less and 5 GHz bandwidth is for a lower range of area but the frequency is high so the speed is very high.

Let’s say, if there is an internet connection of 60 MB/s bandwidth, then for 2.4 GHz bandwidth, it provides approx 30 to 45 MB/s of bandwidth connection and for 5 GHz bandwidth, it provides approx 50 to 57 MB/s bandwidth.

Applications of Wi-Fi :

Wi-Fi has many applications, it is used in all the sectors where a computer or any digital media is used, also for entertaining Wi-Fi is used. Some of the applications are mentioned below – 

Accessing Internet: Using Wi-Fi we can access the internet in any Wi-Fi-capable device wirelessly.

We can stream or cast audio or video wirelessly on any device using Wi-Fi for our entertainment.

We can share files, data, etc between two or more computers or mobile phones using Wi-Fi, and the speed of the data transfer rate is also very high. Also, we can print any document using a Wi-Fi printer, this is very much used nowadays.

We can use Wi-Fi as **HOTSPOTS** also, it points Wireless Internet access for a particular range of area. Using Hotspot the owner of the main network connection can offer temporary network access to Wi-Fi-capable devices so that the users can use the network without knowing anything about the main network connection. Wi-Fi adapters are mainly spreading radio signals using the owner network connection to provide a hotspot.

Using Wi-Fi or WLAN we can construct simple wireless connections from one point to another, known as Point to point networks. This can be useful to connect two locations that are difficult to reach by wire, such as two buildings of corporate business.

One more important application is **VoWi-Fi**, which is known as **voice-over Wi-Fi**. Some years ago telecom companies are introduced VoLTE (Voice over Long-Term Evolution ). Nowadays they are introduced to VoWi-Fi, by which we can call anyone by using our home Wi-Fi network, only one thing is that the mobile needs to connect with the Wi-Fi. Then the voice is transferred using the Wi-Fi network instead of using the mobile SIM network, so the call quality is very good. Many mobile phones are already getting the support of VoWi-Fi.

Wi-Fi in offices: In an office, all the computers are interconnected using Wi-Fi. For Wi-Fi, there are no wiring complexities. Also, the speed of the network is good. For Wi-Fi, a project can be presented to all the members at a time in the form of an excel sheet, ppt, etc. For Wi-Fi, there is no network loss as in cable due to cable break.

Also using W-Fi a whole city can provide network connectivity by deploying routers at a specific area to access the internet. Already schools, colleges, and universities are providing networks using Wi-Fi because of its flexibility.

Wi-Fi is used as a positioning system also, by which we can detect the positions of Wi-Fi hotspots to identify a device location.

Types of Wi-Fi:

Wi-Fi has several types of standards, which are discussed earlier, here just the name of the standards are defined,

|  |  |  |
| --- | --- | --- |
| Standards | Year of Release | Description |
| Wi-Fi-1 (802.11b) | 1999 | This version has a link speed from 2Mb/s to 11 Mb/s over a 2.4 GHz frequency band |
| Wi-Fi-2 (802.11a) | 1999 | After a month of release previous version, 802.11a was released and it provide up to 54 Mb/s link speed over 5 Ghz band |
| Wi-Fi-3 (802.11g) | 2003 | In this version the speed was increased up to 54 to 108 Mb/s over 2.4 GHz |
| 802.11i | 2004 | This is the same as 802.11g but only the security mechanism was increased in this version |
| 802.11e | 2004 | This is also the same as 802.11g, only Voice over Wireless LAN and multimedia streaming are involved |
| Wi-Fi-4 (802.11n) | 2009 | This version supports both 2.4 GHz and 5 GHz radio frequency and it offers up to 72 to 600 Mb/s speed |
| Wi-Fi-5 (802.11ac) | 2014 | It supports a speed of 1733 Mb/s in the 5 GHz band |

Advantages of Wi-Fi

It is a flexible network connection, no wiring complexities. Can be accessed from anywhere in the Wi-Fi range.

It does not require regulatory approval for individual users.

It is salable, can be expanded by using Wi-Fi Extenders.

It can be set up in an easy and fast way. Just need to configure the SSID and Password.

Security in a high in Wi-Fi network, its uses **WPA** encryption to encrypt radio signals.

It is also lower in cost.

It also can provide Hotspots.

it supports roaming also.

Disadvantages of Wi-Fi

Power consumption is high while using Wi-Fi in any device which has a battery, such as mobile, laptops, etc.

Many times there may be some security problems happening even it has encryption. Such as many times has known devices become unknown to the router, Wi-Fi can be hacked also.

Speed is slower than a direct cable connection.

It has lower radiation like cell phones, so it can harm humans.

Wi-Fi signals may be affected by climatic conditions like thunderstorms.

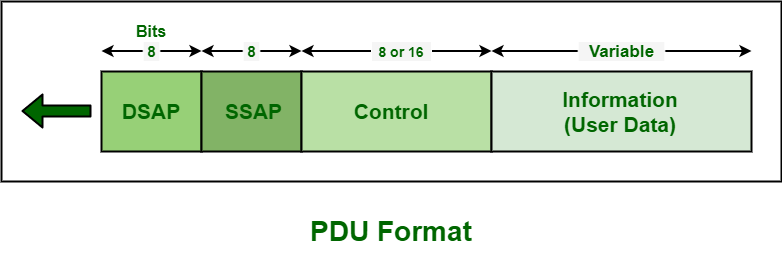
Unauthorized access to Wi-Fi can happen because it does not have a firewall.

To use Wi-Fi we need a router, which needs a power source, so at the time of power cut, we cannot access the internet.

# Logical Link Control (LLC) Protocol Data Unit

Logical Link Control (LLC) is a sublayer that generally provides the logic for the data link as it controls the synchronization, multiplexing, flow control, and even error-checking functions of [DLL (Data Link Layer)](https://www.geeksforgeeks.org/data-link-layer-in-osi-model/). DLL is divided into two sublayers i.e. LLC sublayer and [MAC (Medium Access Control)](https://www.geeksforgeeks.org/mac-full-form/) sublayer.

The basic model of LLC protocols is modeled after the [HDLC (High-Level Data Link Control)](https://www.geeksforgeeks.org/basic-frame-structure-of-hdlc/). These protocols are unacknowledged connectionless service, Connection-oriented service, and acknowledged connectionless service. All of these protocols use the same PDU (Protocol Data Unit) format as shown –



This PDU format basically contains 4 different fields given below – 

Destination Service Access Point (DSAP) Field –   
DSAP is generally an 8-bit long field that is used to represent the logical addresses of the network layer entity meant to receive the message. It indicates whether this is an individual or group address. 

Source Service Access Point (SSAP) Field –   
SSAP is also an 8-bit long field that is used to represent the logical addresses of the network layer entity meant to create a message. It indicates whether this is a command or response PDU. It simply identifies the SAP that has started the PDU. 

Information Field– This field generally includes data or information. 

ControlField– This field identifies and determines the specific PDU and also specifies various control functions. It is an 8 or 16-bit long field, usually depending on the identity of the PDU. It is used for flow and error control. There are basically three types of PDU. Each PDU has a different control field format. These are given below –

Information(I) –   
It generally includes 7-bit sequence number (N(S)) and also a piggybacked sequence number (N(R)). It is used to carry data or information. 

Supervisory(S) –   
It generally includes an acknowledgment sequence number (N(R)) and also a 2-bit S field for three different PDU formats i.e. RNR (Receive Not Ready), RR (Receive Ready), and REJ (Reject). It is generally used for flow and error control. 

Unnumbered(U) –   
It is generally a 5-bit M bit that is used to indicate the type of PDU. It is used for various protocol PDUs. 

Some functions of LLC Sublayer are –

It is responsible to manage and to ensure the integrity of data transmissions.

They provide the logic for the data link.

It also controls the synchronization, multiplexing, error checking or correcting functions, flow control of the DLL.

It also allows multipoint communication over a range of computer networks.