Address Mapping

Address mapping is a process of determining a logical address knowing the physical address of the device and determining the physical address by knowing the logical address of the device. Address mapping is required when a packet is routed from source host to destination host in the same or different network. Why Address Mapping? We know that the Internet is a collection of several physical networks that are interconnected using routers. Now when in an Internet, a source node sends a packet to the destination node the packet has to travel through different physical networks before it is delivered to the destination node. At the network level, any device connected to the network can be identified by its logical address (IP address). However, the device at the physical level is identified by its physical address. The physical address is unique to the local network but not in the universal network such as the Internet. However, the logical address is unique universally. Now why do we require both addresses, we can use only one type of address to identify a host or router in the network. The physical address and the logical address both are different identifiers and we require both of them as the physical address defines the physical connection between source host to destination host whereas the logical address defines routable connection from source host to the destination host and from network to network. So as both physical and logical addresses are essential to route a packet from the source host to the destination host, we require an address mapping mechanism to relate a physical address of the device to its logical address and vice versa.

Types of Address Mapping

There are two kinds of address mapping, static address mapping, and dynamic address mapping. In the section ahead we will discuss both of them in detail.

1. Static Mapping

In static mapping, each device connected to the network maintains a table i.e., routing table which has a list of all the routes from that device to a particular network or hosts. It maintains the network/next hop association i.e., the logical address of next-hop and its corresponding physical address. A source host knows the logical address of the host to which it wants to deliver the packet so it can refer to the routing table to recognize the physical address of the destined host. But the static address mapping has some constraint over the physical address of the device as it changes in certain conditions such as:

1. If a device changes its Network Interface Card (NIC), the physical address of the device also changes. As the physical address is hardcoded on the NIC card at the time of its manufacturing.
2. Some local networks such as Local Talk compel the connected device to change its physical address each time the device turns on.
3. Nowadays there are some third-party apps through which users can change their physical address.

Even the logical address of the device also changes under some circumstances such as:

1. If the host switches the network, this changes the logical address of the host.
2. If you reset your modem, it also results in a change of logical address.
3. If the host gets connected to the network via VPN (Virtual Private Network) then it appears that you.

In such a scenario, if we use static address mapping, more time will be wasted in updating the routing table at each connected device and this will generate overhead on the connected devices which will also affect the performance of the network. A solution to this is dynamic mapping.

2. Dynamic Mapping

In dynamic mapping usually, the source host knows the logical address of the destination host but to deliver the packet to the destined host its physical address is required as at the physical level the device is identified by its physical address. So, the source host uses the protocols to identify the physical address of the destination host. Two protocols are designed for dynamic mapping ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol). ARP protocol determines the physical address of a device knowing its logical address. RARP protocol determines the logical address of a device knowing its physical address. We will discuss how this mapping is done.

Process

1. Mapping Logical Address to Physical Address

When a source host wants to send a packet to the destination host it obtains the logical address of the destination host from the DNS (Domain Name Server). If the packet is at any intermediatory router in the network the logical address of the next-hop router is obtained using the routing table. Now the packet to be sent is encapsulated in the frame at the data link layer as it has to travel

through the physical network and at the physical level the sender would require the physical address of the receiver. So, the source host broadcasts the ARP query packet to all the hosts in the network. The ARP query packet contains the source's physical logical address and the destination's logical address. All the hosts present in the network receive this query packet and but only the target host (destination host) recognize its logical address and prepares an ARP reply packet. Other hosts discard the ARP query packet. The ARP reply packet contains the physical address of the destination host and in this way, the ARP protocol retrieves the physical address for the corresponding logical address. I have described the ARP protocol in brief in our previous content.

2. Mapping Physical Address to Logical Address

To map a physical address of a device to its logical address there are protocols such as RARP, BOOT, DHCP. This RARP protocol is used in the certain scenario such as:

A diskless station is just turned on, it can retrieve its physical address by referring to the NIC interface, but to get its logical address it can RARP protocol.

If an enterprise has a limited IP address, then it assigns an IP address toits hosts on demand for that the host has to IP address for a short time lease.

RARP's working is similar to the working of RARP. The host can get its physical address by reading its NIC card. And to get its logical address the host broadcasts the RARP request packet to its local network. The machine which knows all the IP addresses will respond with the logical address for the host requesting for logical address.

CSMA (Carrier Sense Multiple Access)

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it.

CSMA is based on the principle "sense before transmit" or "listen before talk."

Basic Working

Because data is transmitted in the form of signals and all the station in figure are connected by shared link so if only A and B wants to communicate even then these signals will be received by all stations. Now at the same time when A and B are communicating if C and D wants to communicate the they can't because C will first sense the channel and it will find it busy hence it will not send data.

Now we may think that collision will never occur but the possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit-to-reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received. **Hence here vulnerable time is equal to propagation time.**

Persistence Methods

What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been devised to answer these questions:

a) 1-persistent method used
b) Non persistent method ethernet UITE
c) p-persistent method

1-Persistent: - The 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. Ethernet uses this method.

Nonpersistent: - In the nonpersistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The non persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

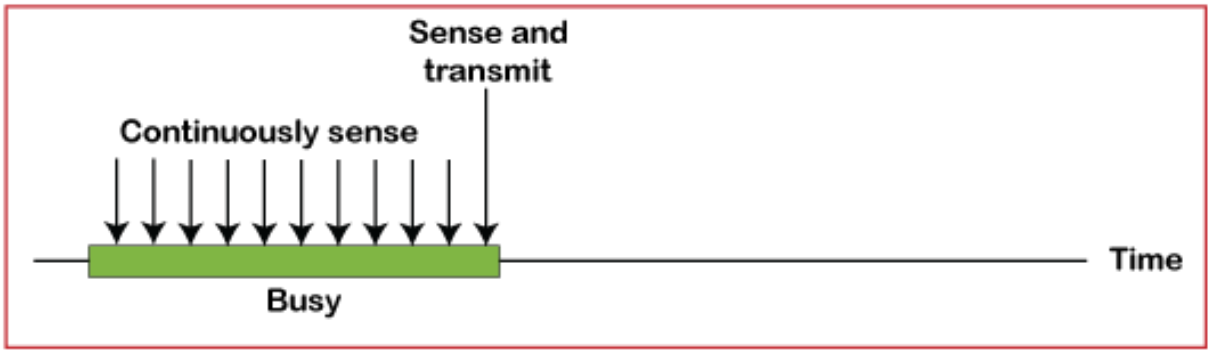
The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency (hence it is best method). In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.

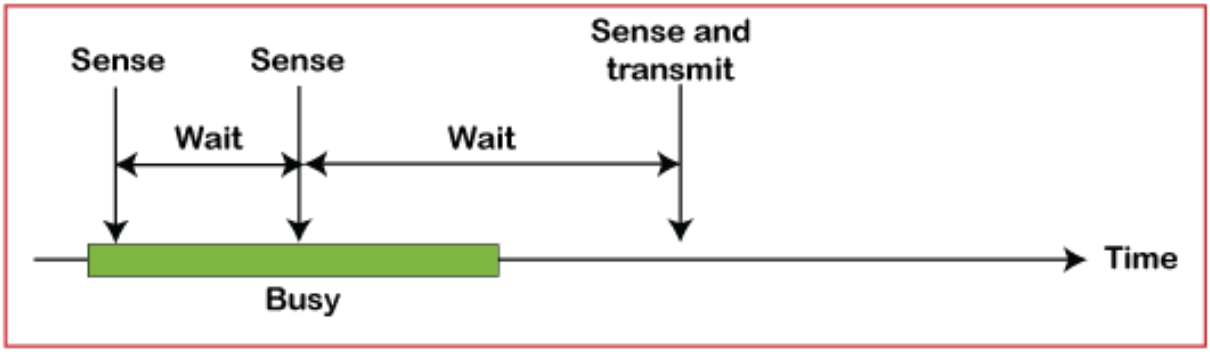
2. With probability q = 1-p, the station waits for the beginning of the next time slot and checks the line again.

a. If the line is idle, it goes to step 1.

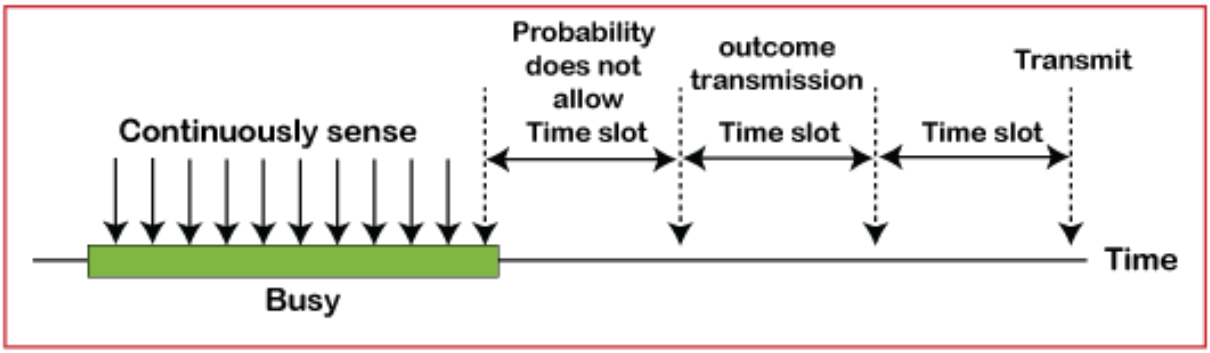
b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.



a. 1-persistent



b. Nonpersistent



c. p-persistent

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

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision. **Hence this protocol is nothing but small extension of CSMA.**

Station does not check for collision after transmission rather it keeps on sending frame and simultaneously it keeps on checking the channel for collision. That means sender needs 2 different ports one for sending data and other for detecting collision. If collision is detected then it immediately stops sending frame.

Obvious Observations

1. **There is no need of ACK** (because if collision is not detected then frame is definitely received by receiver). Please note that this layer is not concerned for error detection i.e., if frame is corrupted then we need to resend it but that is responsibility of LLC and not MAC.

2. **Station does not maintain copy of frame at MAC layer** because it does not need it as station is simultaneously sending frame as well as detecting collision so if collision is not detected that means other station has successfully received the frame.

3. **Minimum frame duration must be 2*Tp**, (Propagation Time) this is because in worst case if the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second, and the effect of the collision takes another time Tp to reach the first. So, the requirement is that the first station must still be transmitting after 2Tp, **so we need minimum size frame i.e., station can't send frame of any arbitrary size and this size depends on bandwidth available and propagation time.**

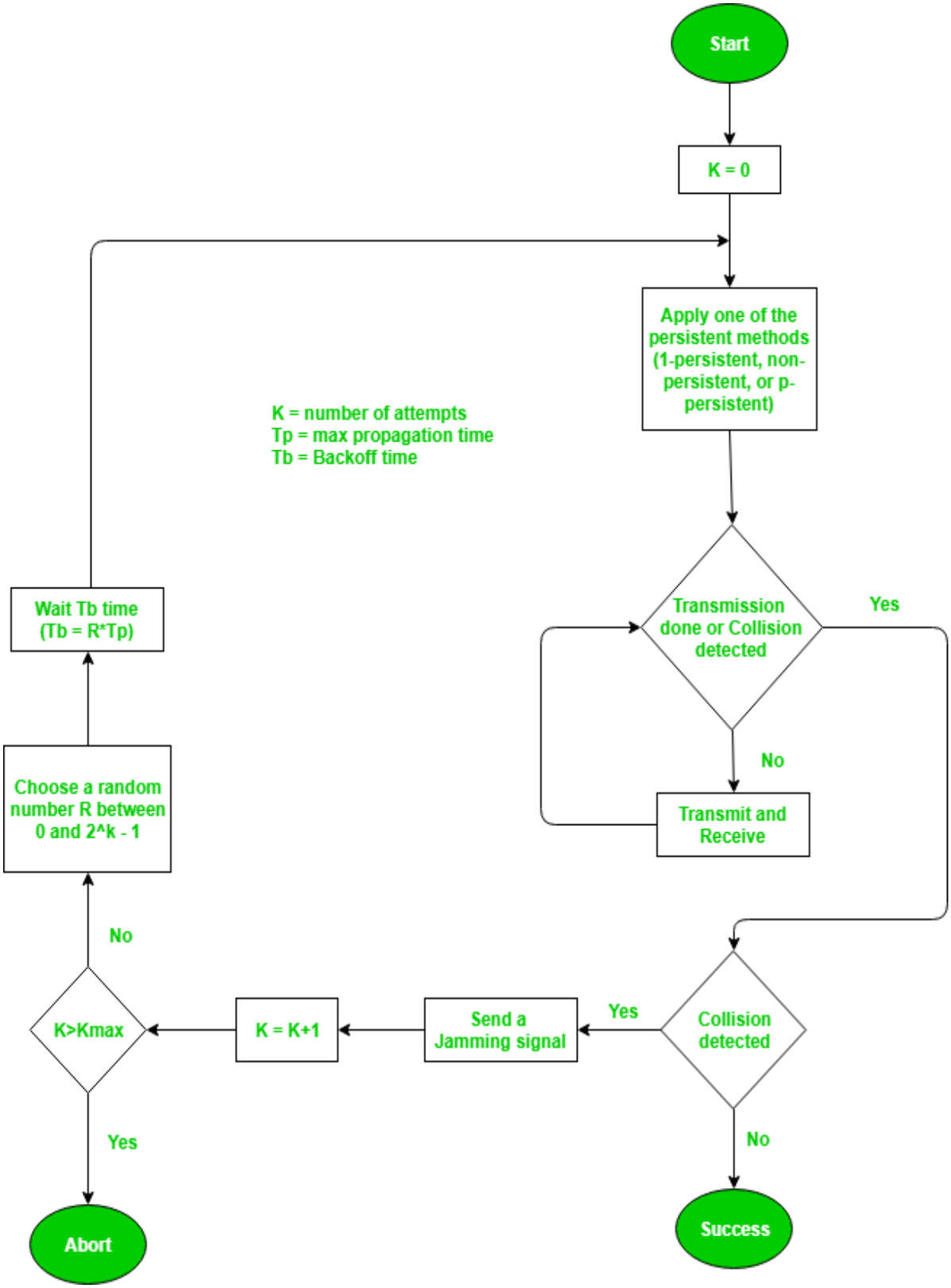
How to detect collision

We can say that the level of energy in a channel can have three values: zero, normal, and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame. At the abnormal level, there is a collision and the level of the energy is twice the normal level. A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.

Throughput

The maximum throughput is 50% when G-1 and 1 persistence method is used. But in case of p persistence method, it is 90% when G is b/w 3 and 8.

Following figure show the general procedure


Start
K = 0
Apply one of the persistent methods (1-persistent, non-persistent, or p-persistent)
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Transmission done or Collision detected
Yes
No
Transmit and Receive
Collision detected
Yes
Send a Jamming signal
K = K+1
K>Kmax
No
Choose a random number R between 0 and 2^k - 1
Wait Tb time (Tb = R*Tp)
Yes
No
Success
Abort

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

CSMA/CD is used in wired network because the received signal has almost the same energy as the sent signal as either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.

However, in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection.

Hence, we need to avoid collisions on wireless networks because they cannot be detected. Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network

Collisions are avoided through the use of CSMA/CA's three strategies:

1. Inter frame space
2. Contention window
3. Acknowledgment

1. Inter frame space

First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately rather it waits for a period of time called the interframe space or IFS.

IFS is the time needed for a signal to reach the given station from the station which is far behind the given station.

This protocol assumes that even though the channel may appear idle when it is sensed, a distant station may have already started transmitting. The distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS

time the channel is still idle, the station can send, but it still needs to wait -a time equal to the contention time (described next).

The IFS time can also be used to prioritize stations or frame types. For example, a station that is assigned a shorter IFS has a higher priority.

Contention Window

The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.

These slots are nothing but transmission time slots as discussed in slotted aloha

Here station keep on checking the channel after each slot if channel is busy them we do not count that slot this means that if random number chosen is 4 then station actually waits for 4 empty slots.

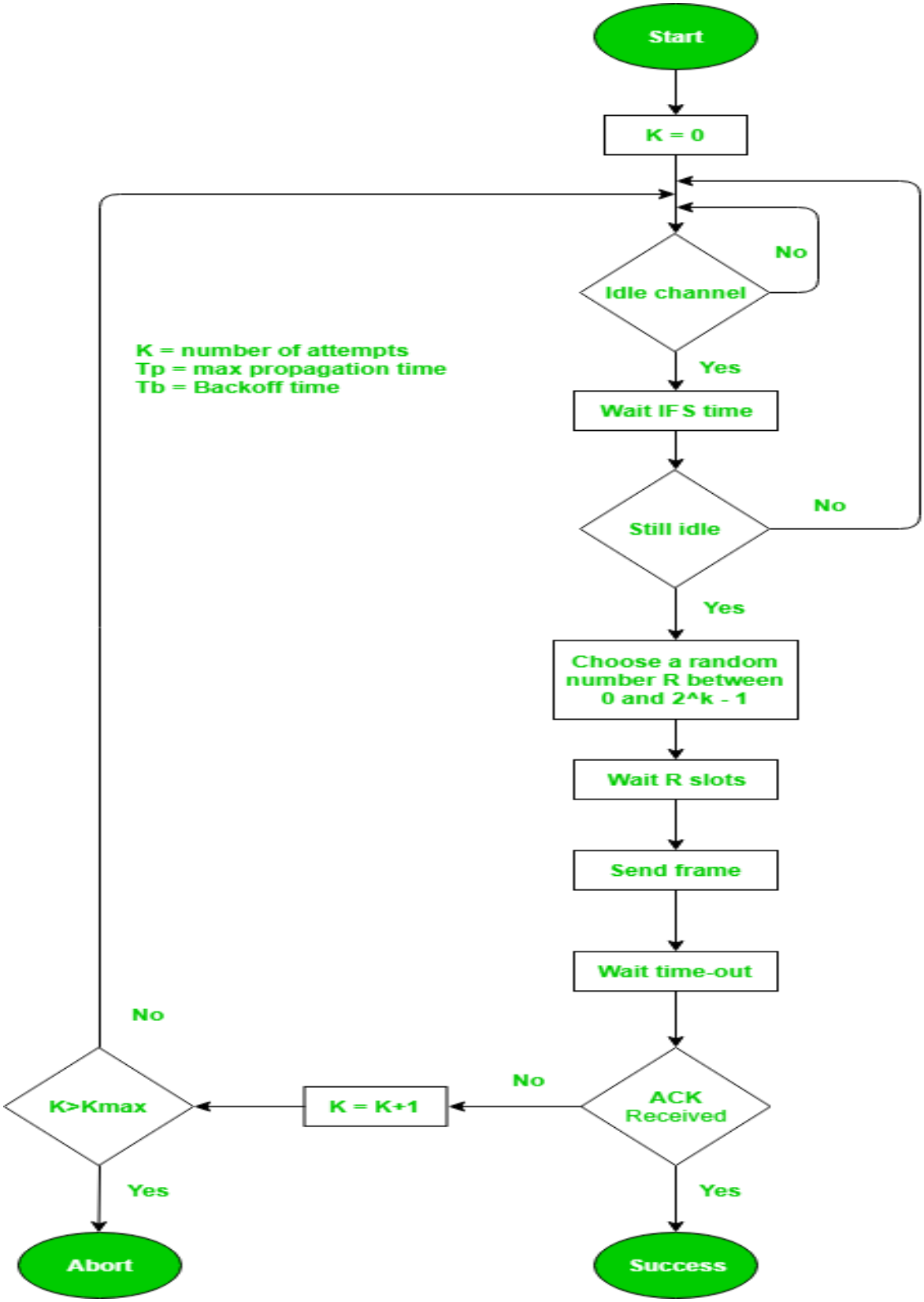
The number of slots in the-window changes according to the binary exponential back-off strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

Acknowledgment

With all these precautions, there still may be a collision resulting in destroyed data.

The positive acknowledgment and the time-out timer can help guarantee that the receiver received the frame.

Following figure gives idea about basic scheme of this protocol.


Start
K = 0
Idle channel
No
Yes
Wait IFS time
Still idle
No
Yes
Choose a random number R between 0 and 2^k - 1
Wait R slots
Send frame
Wait time-out
ACK Received
No
K = K+1
K>Kmax
No
Yes
Abort
Yes
Success
K = number of attempts
Tp = max propagation time
Tb = Backoff time

CONTROLLED ACCESS

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

Another way of saying can be there are primary and secondary stations in n/w primary will control all secondary station

We discuss three popular controlled-access methods

1. Reservation
2. Polling
3. Token passing

TOKEN PASSING

Token passing method is used in token ring LAN and, we will study this LAN Standard for token ring LAN is IEEE 802.5.

As the name suggest here ring topology is used

A special frame is chosen as token of 3-Byte length

This token keeps on rotating in the ring and the station who wants to send the data will **absorb the token and then send the data** (with physical address of sender and receiver)

The data frame will reach the 1st station and this station will match the physical address of destination by itself. If it matches it keep the frame otherwise it will send it to next station.

Now when the frame reaches the destination then the receiver will **produce another copy of same frame** but last 4 bits are set to 1 (indicating that it has received the frame and this will act as ACK). The sender will receive this frame and it now releases the token.

If after specific time ACK does not come then it again send the data but attempts are limited and token remain for each station for specific amount of time and not forever

Token ring allow each station to send only one frame per turn (size of frame is 4500 bytes).

Token may be lost if station having token fails or it may be corrupted by noise in network. So, we need a **monitoring station** and time limit is set normally 10msec. and it must receive frame after this time if it does not then it will produce the new token and circulate it in the network.

Here the main problem is traffic moves in one direction so if any station fails then traffic stops hence in this case, we bye pass the station by automatic switch.

If the destination fails then sender will again receive the frame but now because it is not modified so sender will not assume that receiver has received the frame.

Addressing here is of 48 bits written on NIC card.

Signalling is differential Manchester.

Data rate was originally 4 Mbps but now up to 16 Mbps.

3 Types of Frame

1. Data or command frame (It carry data max. of 4500 bytes)
2. Token frame (3-Byte frame circulating in n/w)
3. Abort frame (used by sender to abort its transmission)

FDDI

FDDI is Fiber Distributed Data Interface

It is type of LAN standardized by ANSI

It also uses **token passing** and uses **dual ring (1st is primary and second used when 1st fails)**

As the name suggest it uses ring made of Fiber optic cable of multimode type and data is converted into light energy by LEDS

The main differences with token ring are

Data rate is 100 Mbps

Station can send data as much as it wants during its time slot but in token ring it was fixed i.e., 4500 bytes

Here we have 2 types of frame S (synchronous) frame and A(asynchronous) frame. S frame has more priority and hence carry real time data like audio video.

A frame has less priority so it carries text data.

FDMA

FDMA is Frequency Division Multiple Access and is DLL technique but FDM is of physical

The main difference b/w multiplexing (physical layer) and multiple access (data link layer) is that station can be present far apart in multiple access but they must be present very near to each other in multiplexing.

In (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time. So even if station is not sending data channel will remain idle.

Each station also uses a band pass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.

TDMA

In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data.

Each station transmits its data in is assigned time slot.

The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot.

This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area. To compensate for the delays, we can insert guard times. Synchronization is normally accomplished by having some synchronization bits (normally referred to as preamble bits) at the beginning of each slot.

TDMA is used in GSM technology.

Please note that TDMA works at DLL but TDM at physical layer.

Code-Division Multiple Access (CDMA)

In CDMA, one channel carries all transmissions simultaneously.

CDMA simply means communication with different codes. For example, in a large room with many people, two people can talk in English if nobody else understands English. Another two people can talk in Chinese if they are the only ones who understand Chinese, and so on. In other words, the common channel, the space of the room in this case, can easily allow communication between several couples, but in different languages (codes).

IEEE started project 802

IEEE started project 802 so that different LANS can be interconnected. In 1985, the Computer Society of the IEEE (Institute of Electrical and Electronics Engineers) started a project, called Project 802; to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model.

Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802.

IEEE subdivided the data link layer into two sub layers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC).

In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sub layer called the logical link control.

Framing is handled in both the LLC sub layer and the MAC sub layer. The LLC provides one single data link control protocol for all IEEE LANS which is known as PDU (protocol data unit and is similar to HDLC).

In this way, the LLC is different from the media access control sub layer, which provides different protocols for different LANs for e.g., Ethernet, token ring, token bus etc.

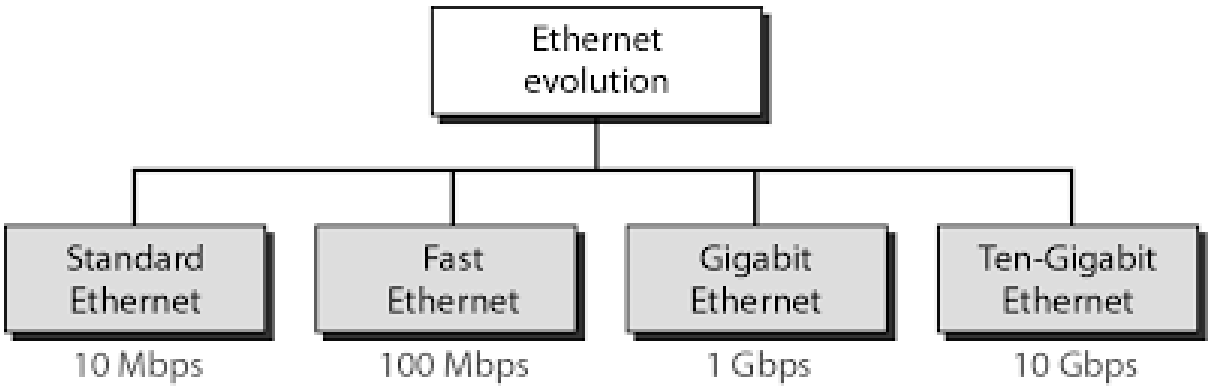
we must remember the following standard numbers

IEEE project 802.1	Bridged LAN
IEEE project 802.2	LLC
IEEE project 802.3	Ethernet
IEEE project 802.4	Token Bus
IEEE project 802.5	Token Ring
IEEE project 802.6	DQDB (Distributed Queue Dual Bus)
IEEE project 802.11	WLAN

Ethernet Evolution

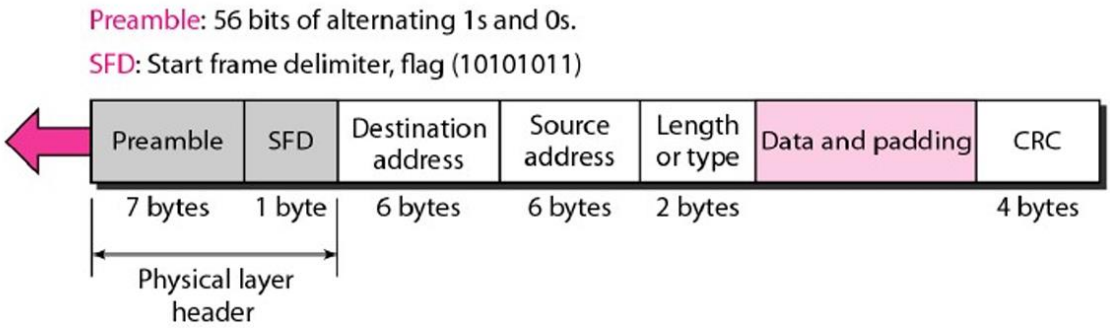
MAC Sublayer

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



1. Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers.



Preamble: The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0sand 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse.

Start frame delimiter (SFD). The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

Destination address (DA). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.

Source address (SA). The SA field is also 6 bytes and contains the physical address of the sender of the packet.

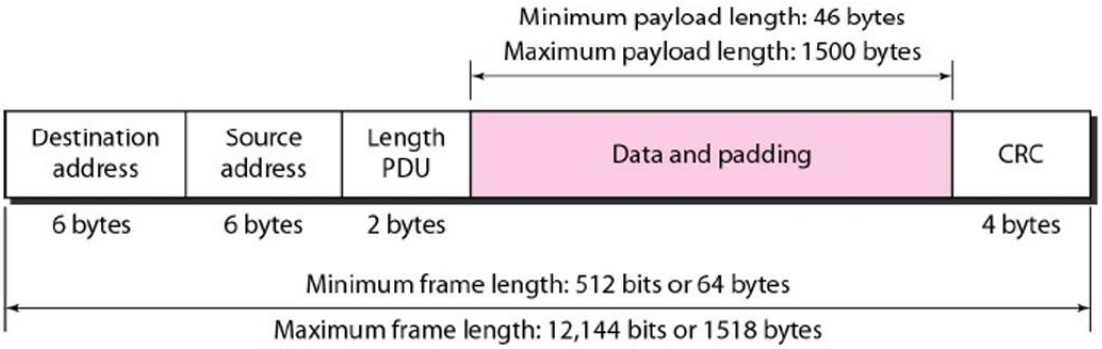
Length or type. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame.

Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

CRC. The last field contains error detection information, in this case a CRC-32.

2. Frame Length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer, then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.



The standard defines the maximum length of a frame as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons.

First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer.

Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send (because the bandwidth was very less at that time).

3. Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical (MAC) address. As shown in Figure 13.4, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

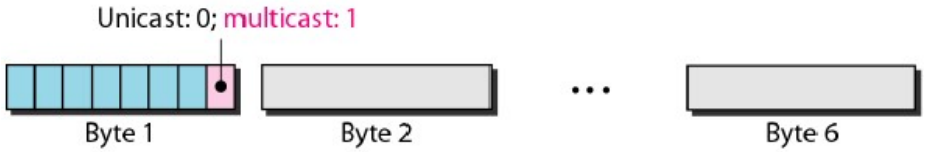
Unicast, Multicast, and Broadcast Addresses Data is transmitted over a network by three simple methods i.e., Unicast, Broadcast, and Multicast. So, let's begin to summarize the difference between these three:

Unicast: from one source to one destination i.e. One-to-One

Broadcast: from one source to all possible destinations i.e. One-to-All

Multicast: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many.

- A source address is always a unicast address as the frame comes from only one station.
- The destination address, however, can be unicast, multicast, or broadcast.
- How to distinguish a unicast address from a multicast address. If the least significant bit of 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; the relationship between the sender and the receiver is one-to-one.
- A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many.
- The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight 1s.

Example

Define the type of the following destination addresses:

1. 4A:30:10:21:10:1A
2. 47:20:1B:2E:08:EE
3. FF:FF:FF:FF:FF:FF

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010 (even).

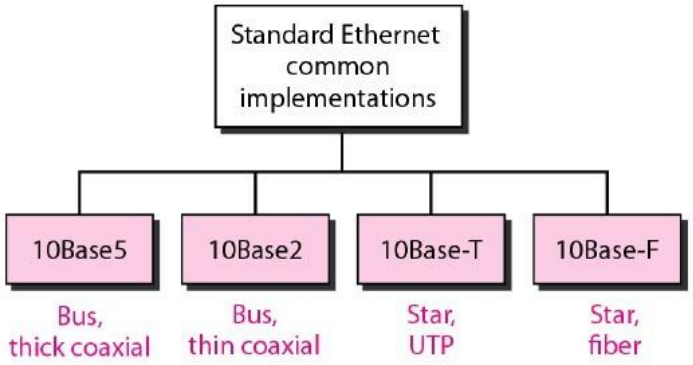
b. This is a multicast address because 7 in binary is 0111 (odd).

c. This is a broadcast address because all digits are F's.

The way the addresses are sent out on line is different from the way they are written in hexadecimal notation. The transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last. This means that the bit that defines an address as unicast or multicast arrives first at the receiver.

Categories of Standard Ethernet

The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in Figure.

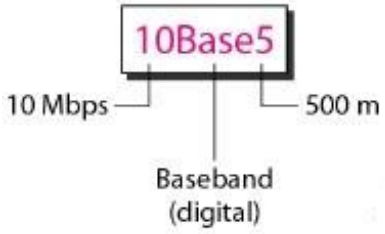


Encoding and Decoding

All standard implementations use digital signalling (baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data.

- **10Base5: Thick Ethernet**

The first implementation is called **10Base5, 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. 10Base5 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.



The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable. The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive degradation of the signal. If a

length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

- **10Base2: Thin Ethernet**

The second implementation is called 10Base2, thin Ethernet, or Cheaper net. 10Base2 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.

Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

- **10Base-T: Twisted-Pair Ethernet**

The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable. Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

- **10Base-F: Fiber Ethernet**

Although there are several types of optical Fiber 10-Mbps Ethernet, the most common is called 10Base-F. 10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two Fiber-optic cables.

Summary

Table shows a summary of Standard Ethernet implementations.

Characteristics	***10Base5***	***10Base2***	***10Base-T***	***10Base-F***
Media	Thick Coaxial Cable	Thin Coaxial Cable	2UTP	2Fiber
Maximum length	500m	185m	100m	2000m
Line encoding	Manchester	Manchester	Manchester	Manchester
Transmission Mode	Half duplex	Half Duplex	Full Duplex	Full Duplex
Topology	Bus	Bus	Star	Star

Fast Ethernet (IEEE 802.3u)

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:

a. Upgrade the data rate to 100 Mbps.

b. Make it compatible with Standard Ethernet.

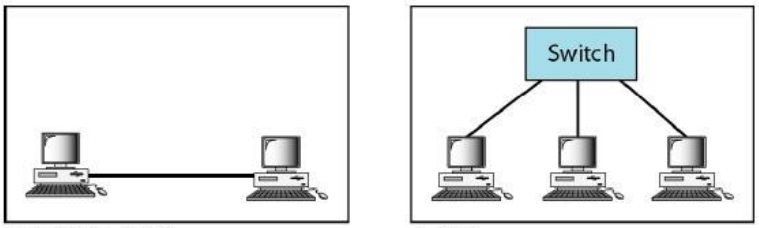
c. Keep the same 48-bit address.

d. Keep the same frame format.

e. Keep the same minimum and maximum frame lengths.

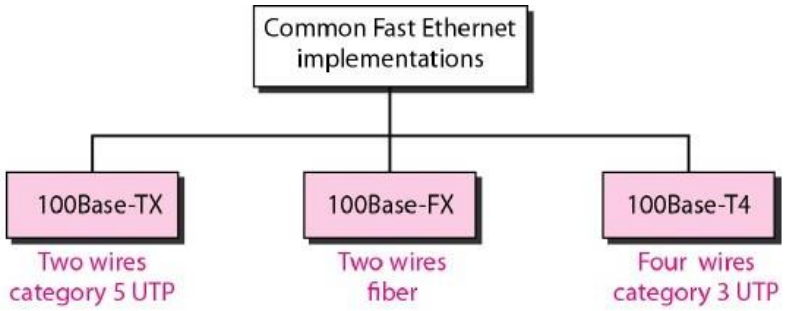
Topology

Fast Ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the centre, as shown in Figure



Implementation

Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire. The two-wire implementation can be either category 5 UTP (100Base-TX) or Fiber-optic cable (100Base-FX). The four-wire implementation is designed only for category 3 UTP (100Base-T4).



Characteristics	100Base-TX	100Base-FX	100Base-T4
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100m	100m	100m
Line encoding	MLT-3	NRZ-I	8B/6T

Gigabit Ethernet(IEEE 802.3z)

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:

a. Upgrade the data rate to 1 Gbps.

b. Make it compatible with Standard or Fast Ethernet.

c. Use the same 48-bit address.

d. Use the same frame format.

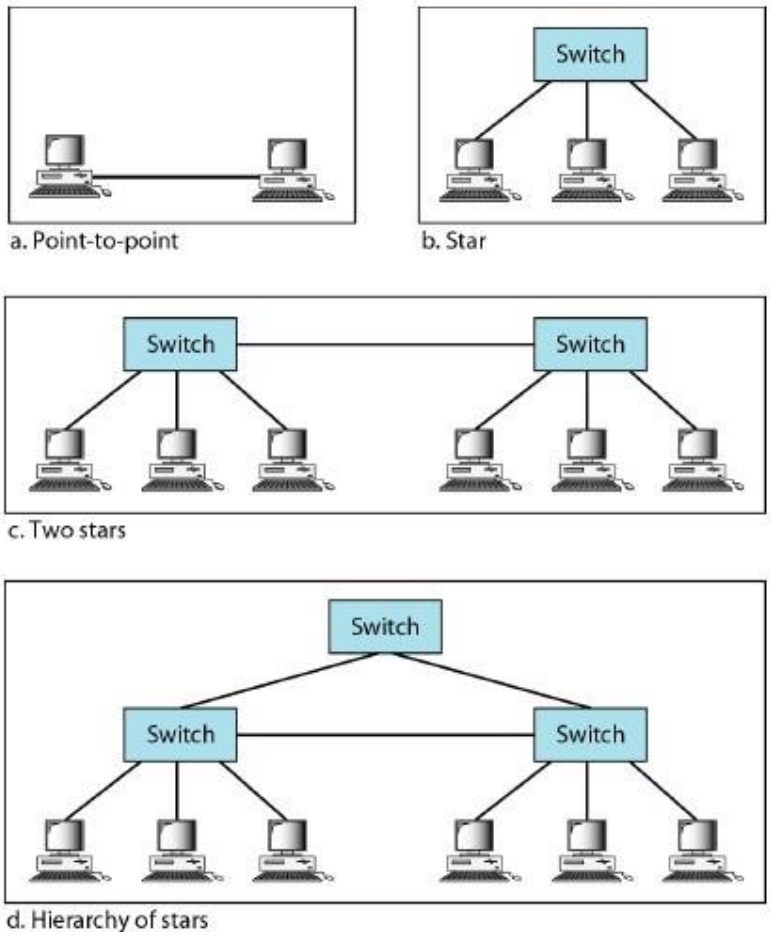
e. Keep the same minimum and maximum frame lengths.

f. To support autonegotiation as defined in Fast Ethernet.

Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full- duplex. Almost all implementations of Gigabit Ethernet follow the full-duplex approach.

Topology

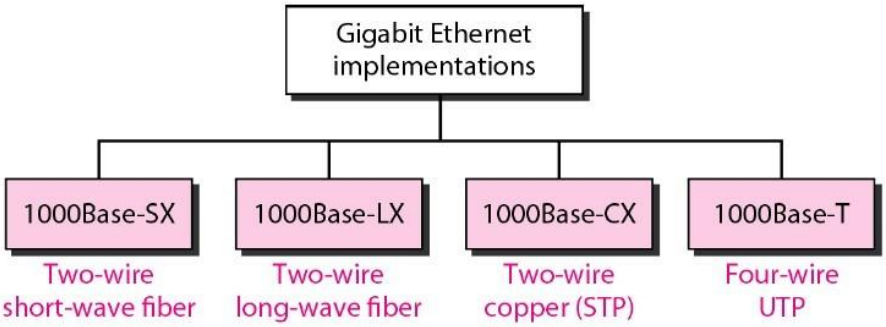
Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. Another possible configuration is to connect several star topologies or let a star topology be part of another as shown in Figure.



Topologies of Gigabit Ethernet

Implementation

Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation. The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX). The four-wire version uses category 5 twisted-pair cable (1000Base-T). In other words, we have four implementations, as shown in Figure.



Gigabit Ethernet implementations

Characteristics	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T
Media	Fiber Short wave	Fiber Long wave	STP	CAT 5 UTP
Number of wires	2	2	2	4
Maximum length	550m	5000m	25m	100m
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Summary of Gigabit Ethernet implementations

Ten-Gigabit Ethernet(IEEE 802.3ae)

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae. The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

a. Upgrade the data rate to 10 Gbps.
b. Make it compatible with Standard, Fast, and Gigabit Ethernet.
c. Use the same 48-bit address.
d. Use the same frame format.
e. Keep the same minimum and maximum frame lengths.
f. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
g. Make Ethernet compatible with technologies such as Frame Relay and ATM.

Ten-Gigabit Ethernet operates only in full duplex mode which means there is no need for contention; CSMA/CD is not used in Ten-Gigabit Ethernet.

Implementation

Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase-E. Table shows a summary of the Ten-Gigabit Ethernet implementations:

Characteristics	10GBase-S	10GBase-L	10GBase-E
Media	Short-wave 850-nm multimode	Long-wave 1310-nm Single mode	Extended 1550-mm Single mode
Maximum Length	300m	10km	40km

WAN Technologies

WAN is wide area network which is nothing but an internetwork i.e multiple LANs are connected with routers. Here we are using routers as connecting device because we need logical addressing as well because 2 computers in different LANS can have same physical address.

And logical address can be seen by routers (layer 3 device) so we need routers as connecting devices. There are several WAN technologies available today but we will study 3 of them

1. X.25 is a DLL standard
2. Frame relay(DLL standard)
3. ATM(separate data model)

X.25

1. X.25 is a DLL standard but because it is a WAN technology so n/w layer is also needed (for logical addressing). But we are calling it as DLL standard because the main layer used in this technology is DLL.

2. Just like X.21(physical layer standard), standard for X.25 was also given by ITU-T.

3. In 1970 it was launched and it was the first public data network

4. It was connection oriented scheme. That means the computer must establish a connection with remote computer i.e. place a telephone call. This connection was given a unique number DLCI (Data Link Connection Identifier) so that data can be transferred. Unique number is given because at a time there can be many computers which are connected to remote computer.

5. Data packets were simple having 3 bytes header and upto 128 bytes data (so packets were of variable length)

6. Header contains DLCI(12 bits),sequence number, ACK number etc.

7. Data rate was **64 Kbps.**

8. Data rate was less because channels were not reliable at that time so this protocol needs excessive flow and error control.

Frame Realy

1. In 1980's it was developed.

2. It was connection oriented scheme ile virtual circuit was established and then data was transferred

3. This technology needs less flow and error control because channels were reliable at that time and hence data rate was dependent on channel bandwidth i.e. if Tl lines then 1.5 Mbps

4. Rest every thing was same as X.25. Except that it strictly works on only first 2 layer of OSI model i.e DLL and physical, n/w layer is not included here

ATM (Asynchronous Transfer Mode)

It was connection oriented scheme.

In 1980's computer networks start emerging and at that time there were 3 networks.

1. Telephone N/W
2. T.V. N/W
3. Computer N/W

At that time telephone n/w were fully developed but computer n/w were start emerging And sooner telephone companies realize the fact that profit margin in telephone will decrease due to heavy competition.

So telephone companies started thinking of integrating data n/w and telephone n/w. It was a big challenge at that time because technology was not advanced.

And then ITU-T gave its recommendation in the form of ATM.

1. Universal Service

It is very important and first goal of ATM. It means that any user can share voice, video or data with any other user in any part of the world. It was very difficult because even telephone n/w were not present at that time in entire world and ATM was going to run on this telephone n/w.

2. Support for all services

It means that ATM n/w must support audio, video and data on a single unified network.

3. Guaranteed Services

It means that if A is sending data to B then only B must receive it i.e. no other user can receive it and there should be guarantee that B has received it.

4. Low cost

Achieving all the above 3 goals were very difficult at that time but this was another imposible goal i.e. low cost. So it was just like day dreaming at that time.

Features of ATM

1. Transmit all types of data in small fixed sized packet known as cells.

2. **Size of each cell was 53 bytes**

3. Header of each cell was of 5 bytes and 48 bytes of payload was present

4. So approx 10% was overhead hence we can't achieve more than 90% throughput.

5. Cells are transmitted asynchronously i.e. there was no fixed delay b/w sending packets. Like 1st packet after 10 msec 2nd after 100 msec and so on

6. N/W was connection oriented i.e. first connection was established and then data was transferred and all packets will travel from same path it at all.

7. ATM was independent of transmission media i.e. it can run on UTP or fiber optic cable or any wireless media.

8.. We can send any type of data in these cells..

9. Speed of the n/w was very high i.e. upto **655 Mbps.**

Virtual Connection

Because it is connection oriented scheme so we must understand how this connection is identified and established.

Connection between two endpoints is accomplished through:

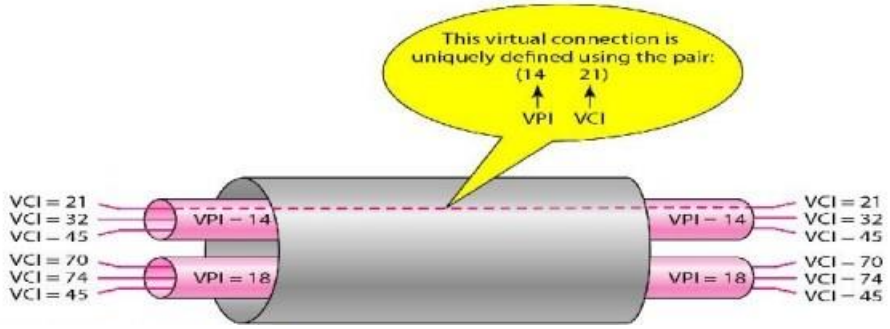
1. Transmission Paths (TPs)
2. Virtual paths (VPS)
3. Virtual Circuits (VCs)

A transmission path (TP) is the physical connection (wire, cable, satellite, and so on) between an endpoint and a switch or between two switches. Think of two switches as two cities. A transmission path is the set of all highways that directly connect the two cities.

A transmission path is divided into several **virtual paths.** A virtual path (VP) provides a connection or a set of connections between two switches. Think of a

virtual path as a highway that connects two cities. Each highway is a virtual path; the set of all highways is the transmission path.

Cell networks are based on **virtual circuits (VCs).** All cells belonging to a single message follow the same virtual circuit and remain in their original order until they reach their destination. Think of a virtual circuit as the lanes of a highway (virtual path).

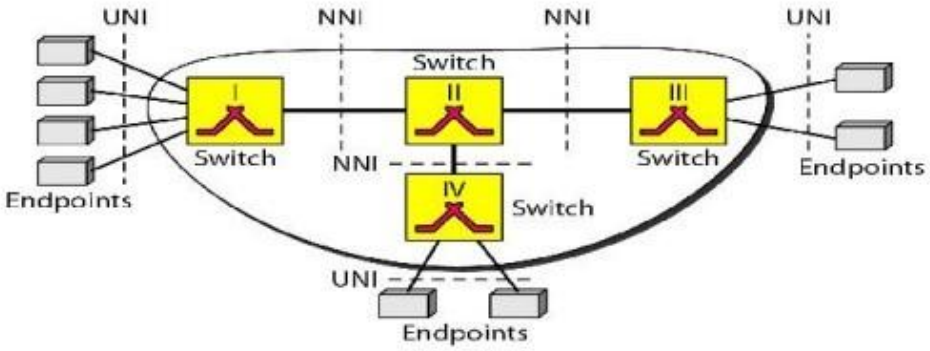


Identifiers

In a virtual circuit network, to route data from one endpoint to another, the virtual connections need to be identified. For this purpose, the designers of ATM created a hierarchical identifier with two levels: a virtual path identifier (VPI) and a virtual-circuit identifier (VCI). The VPI defines the specific VP, and the VPI defines a particular VC inside the VP. The VPI is the same for all virtual connections that are bundled (logically) into one VP.

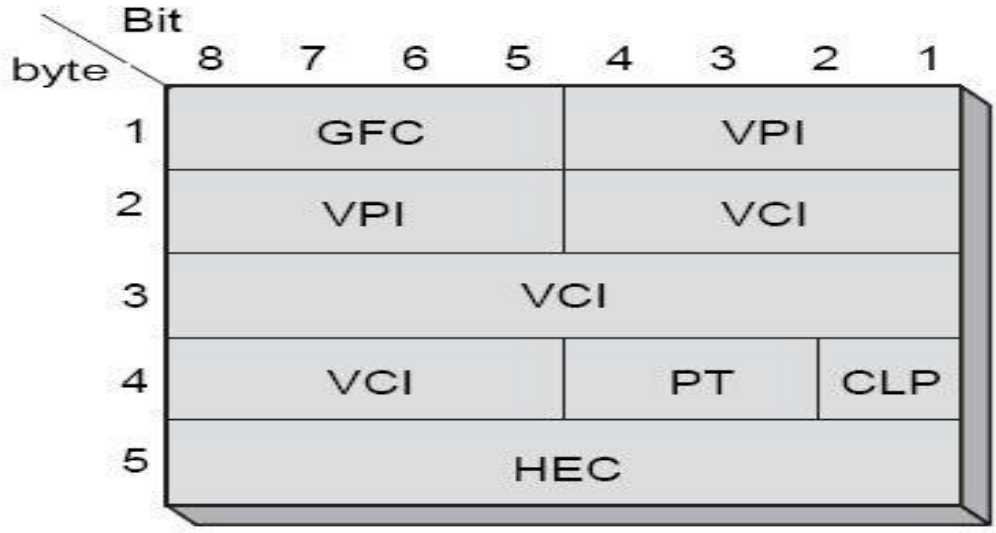
Architecture

ATM is a cell-switched network. The user access devices, called the endpoints, are connected through a user-to-network interface (UNI) to the switches inside the network. The switches are connected through network-to-network interfaces (NNIs).

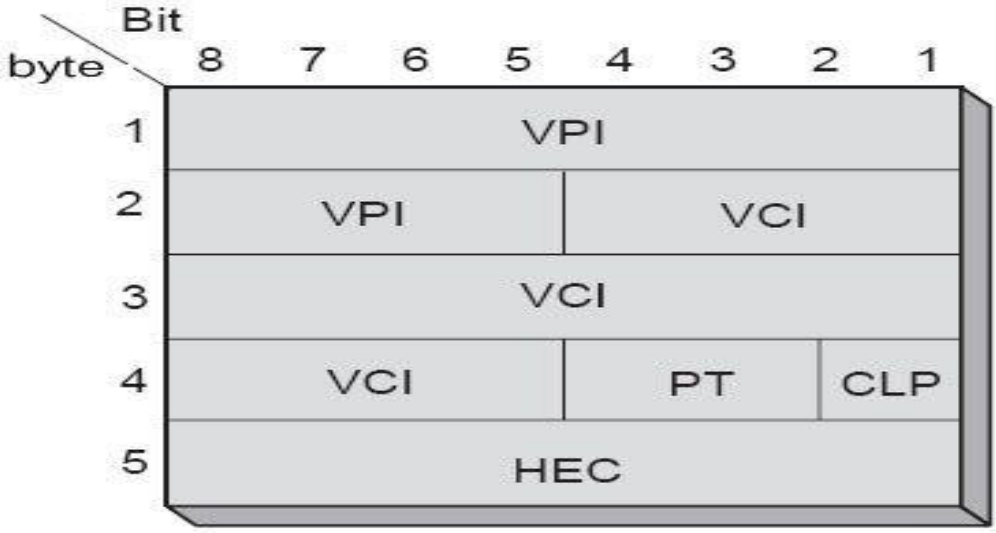


So cells present b/w end points and switch are known as UNI cells and cells present b/w 2 switches are known as NNI cells.

Cell structure



Structure of the ATM cell on the UNI



Structure of the ATM cell of the NNI

Generic flow control (GFC). The 4-bit GFC field provides flow control at the UNI level. The ITU-T has determined that this level of flow control is not necessary at the NNI level. In the NNI header, therefore, these bits are added to the VPI. The longer VPI allows more virtual paths to be defined at the NNI level.

Virtual path identifier (VPI). The VPI is an 8-bit field in a UNI cell and a 12-bit field in an NNI cell (see above figure).

Virtual circuit identifier (VCI). The VCI is a 16-bit field in both frames. So a virtual circuit is identified by 24 bit in UNI cell and 28 bit in NNI cell. So most of the part of header is VPI and VCI.

Payload type (PT). In the 3-bit PT field, the first bit defines the payload as user data or managerial information. The interpretation of the last 2 bits depends on the first bit.

Cell loss priority (CLP). The 1-bit CLP field is provided for congestion control. A cell with its CLP bit set to 1 must be retained as long as there are cells with a CLP of 0.

Header error correction (HEC). The HEC is a code computed for the first 4 bytes of the header. It is a CRC with the divisor x^8+x^2+x+1 that is used to correct single-bit errors and a large class of multiple-bit errors.

Switiching in ATM

ATM uses switches to route the cell from a source endpoint to the destination endpoint. A switch routes the cell using both the VPls and the VCls. The routing requires the whole identifier. Figure above shows how a VPC switch routes the cell. A cell with a VPI of 153 and VCI of 67 arrives at switch interface (port) 1. The switch checks its switching table, which stores six pieces of information per row: arrival intetface number, incoming VPI, incoming VCI, corresponding outgoing interface number, the new VPI, and the new VCL The switch finds the entry with the interface 1. VPI 153, and VCI 67 and discovers that the combination conresponds to output interface 3, VPI 140, and VCI 92. It changes the VPI and VCI in the header to 140 and 92, respectively, and sends the cell out through interface 3.

So every packet of same connection will travel through same path. The basic concept is same as that of virtual circuit switching as studied earlier.

ATM LAYERS

The ATM standard defines three layers. They are, from top to bottom

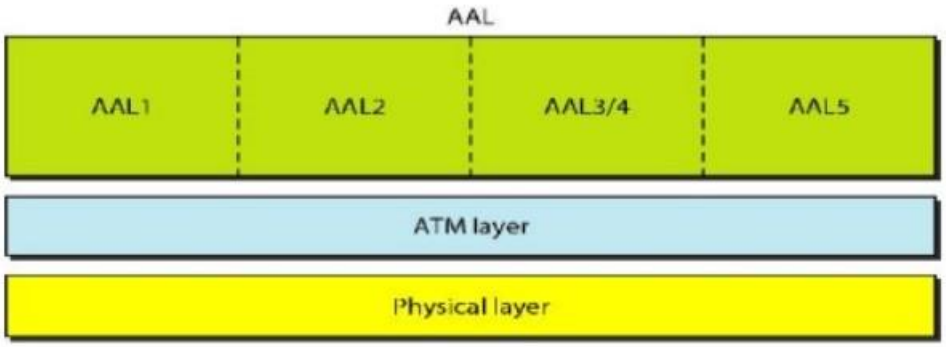
1. Physical layer (layer number 1)

2. ATM layer (layer number 2)

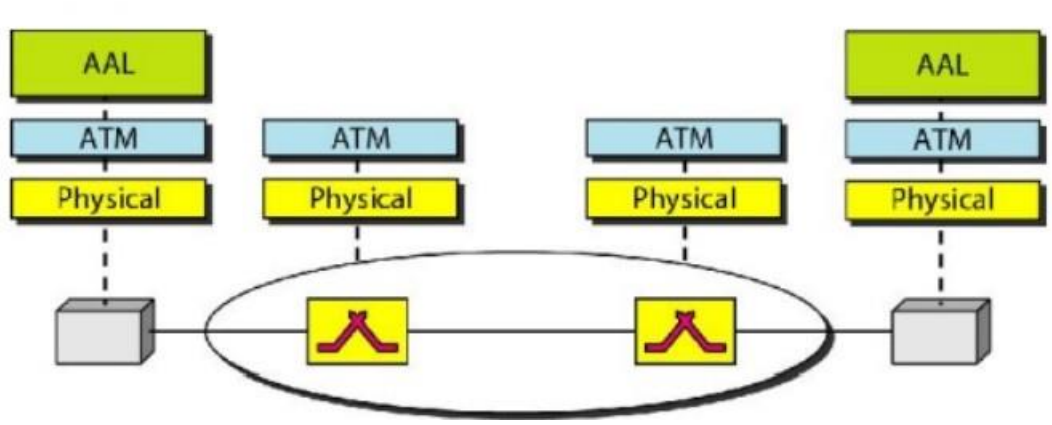
3. Application Adaptation Layer (layer number 3)

It is important to note that ATM is a completely different n/w model it is not based on OSI or TCP/IP.

So we can't say that ATM is which layer standard



Layers Used in End Devices



So AAL is present in end devices and nodes or switches have only 2 layers.

AAL

AAL is further divided into 2 sub layers

1. Convergence sub layer(CS)
2. Segmentation and reassembly sub layer(SAR)

Convergence sub layer(CS)
It offer different kind of services to different applications for e.g.

CBR(Constant Bit Rate)- It is suitable for real time data like audio and video (multimedia). Because here the bit rate remains constant. Obviously it is a costly service

ABR(Available Bit Rate)- It is suitable for text messages so it hardly matter what is the bandwidth available we can easily send text messages. Obviously it is not a costly service.

VBR(Variable Bit Rate)-With this kind of service we can send multimedia messages by using constant bit rate and text messages by available bit rate. So it less costly service then CBR but more costlier then ABR.

Based on these services we have divided AAL into 4 categories. AALI, AAL2, AAL3/4, AAL5.

Segmentation And Reassembly Sub Layer(SAR)
This layer is responsible for chopping large messages at sender side into small packets of 48 bytes this is known as **Segmentation.**

And small packets into large message i.e. reverse process at receiver side and this is known as **Reassembly.**

So we can say that AAL is just like application layer of TCP/IP or OSI model.

ATM layer

This layer is just like DLL and N/W layer of OSI model.

So this layer is responsible for switching, congestion control, and cell header processing.

Physical Layer

This layer is also divided into 2 sub layers.

1. Transmission Convergence Sub Layer
2. Physical Medium Dependent Sub Layer

Transmission Convergence Sub Layer
This layer is responsible for:-

1. Header Error Correction (HEC) generation and verification.

2. Header verification

3. Detect cell boundaries

4. Insert ideal cells in case of CBR if no data is generated in specified time.

Physical Medium Dependent Sub Layer
This layer is responsible for:-

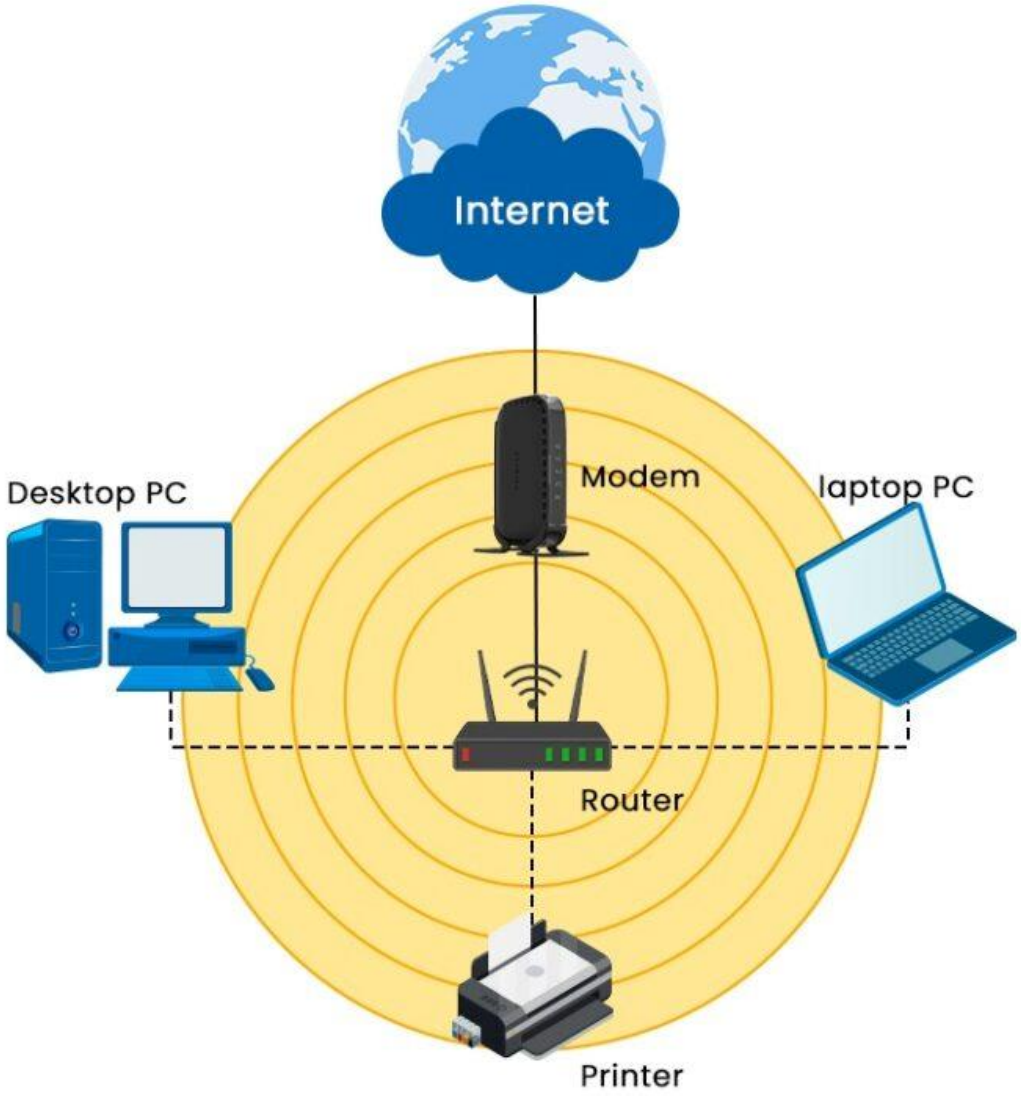
1. Bit timing/duration

2. Physical media and its characteristics.

This layer is same as studied earlier in OSI model physical layer like which type of media is used (UTP,optical fiber or wireless) and its characteristics like single mode or multimode optical fiber etc.

Wireless LAN

A Wireless Local Area Network (WLAN), also known as a Wireless LAN, is a network comprising two or more computing devices that communicate through radio waves without the need for physical connections. This stands in contrast to a local area network (LAN) that employs wired connectivity, whereby every computer within the network is physically linked to the network switch or hub via an Ethernet cable.

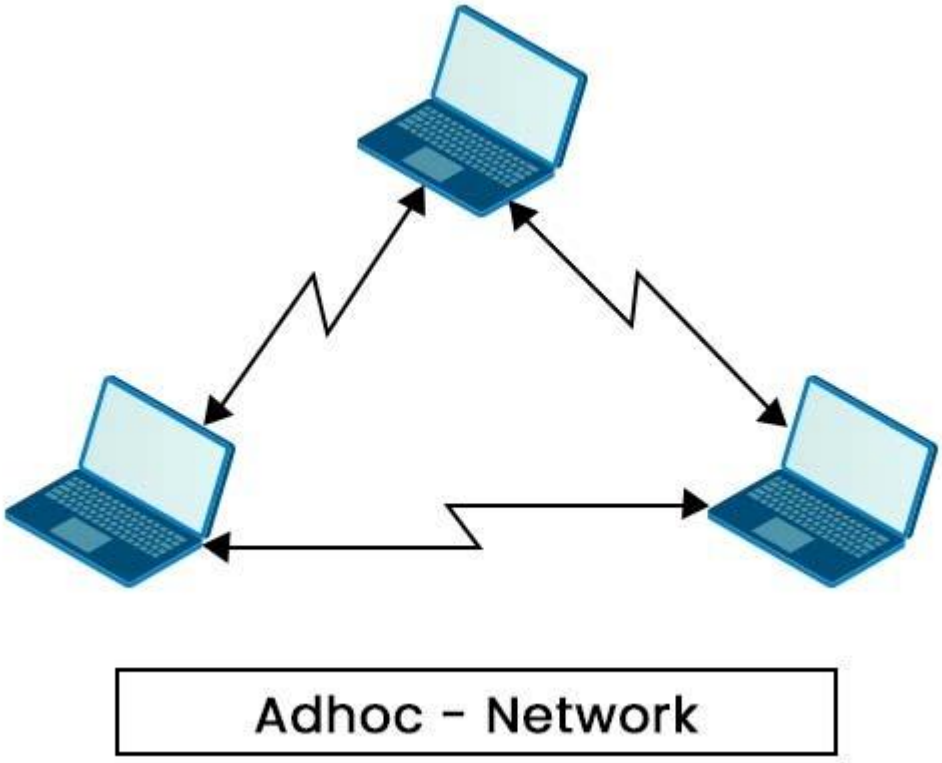


The majority of WLANs are established on the IEEE 802.11 standard.

Wireless LANs are further classified into two categories, these are:

1. **Ad-hoc Wireless LANs**

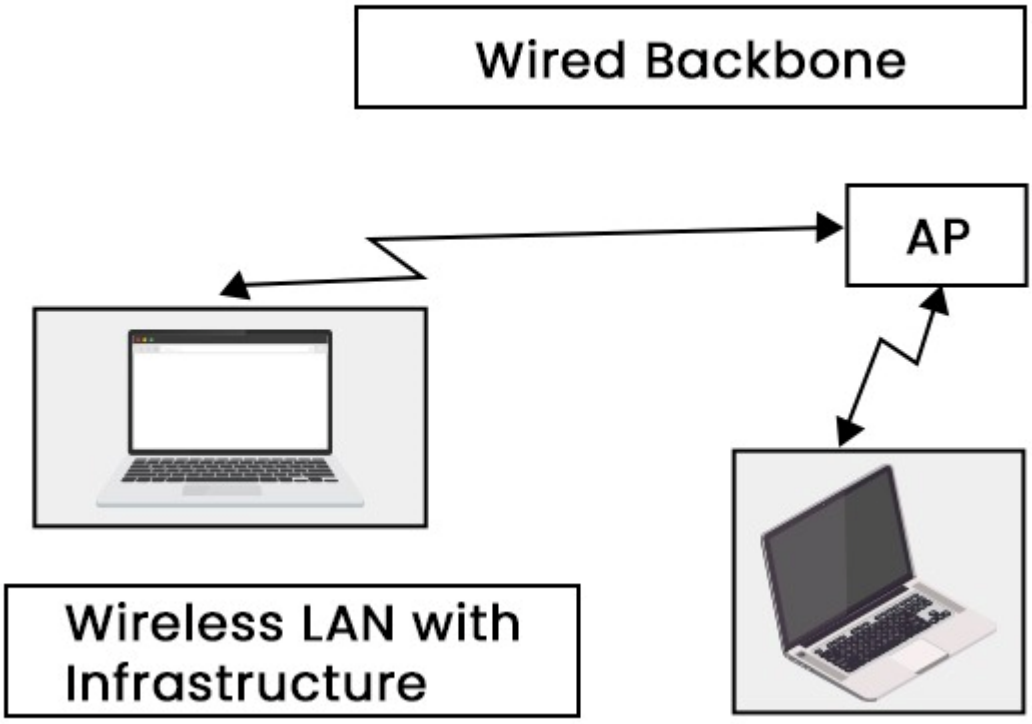
Ad hoc networks are formed by a group of wireless nodes that establish peer-to-peer communication. The ad-hoc mode has been designed to allow communication only among clients within the transmission range, i.e., within the same cell.



If a client wants to communicate outside the cell, then it's a must that one of the cells acts as the gateway and performs routing.

2. Wireless LANs with Infrastructure

Wireless LANs with infrastructure are equipped with a backbone that operates at high speeds and can be wired or wireless. Access points serve as the intermediary between wireless nodes and the wired backbone. The utilization of access points allows the proficient transfer of network resources among wireless nodes.



Before transmitting information, wireless devices such as clients and access points are required to establish a relationship or association. Data exchange between two wireless stations can only occur once an association has been established.

Purpose of WLAN

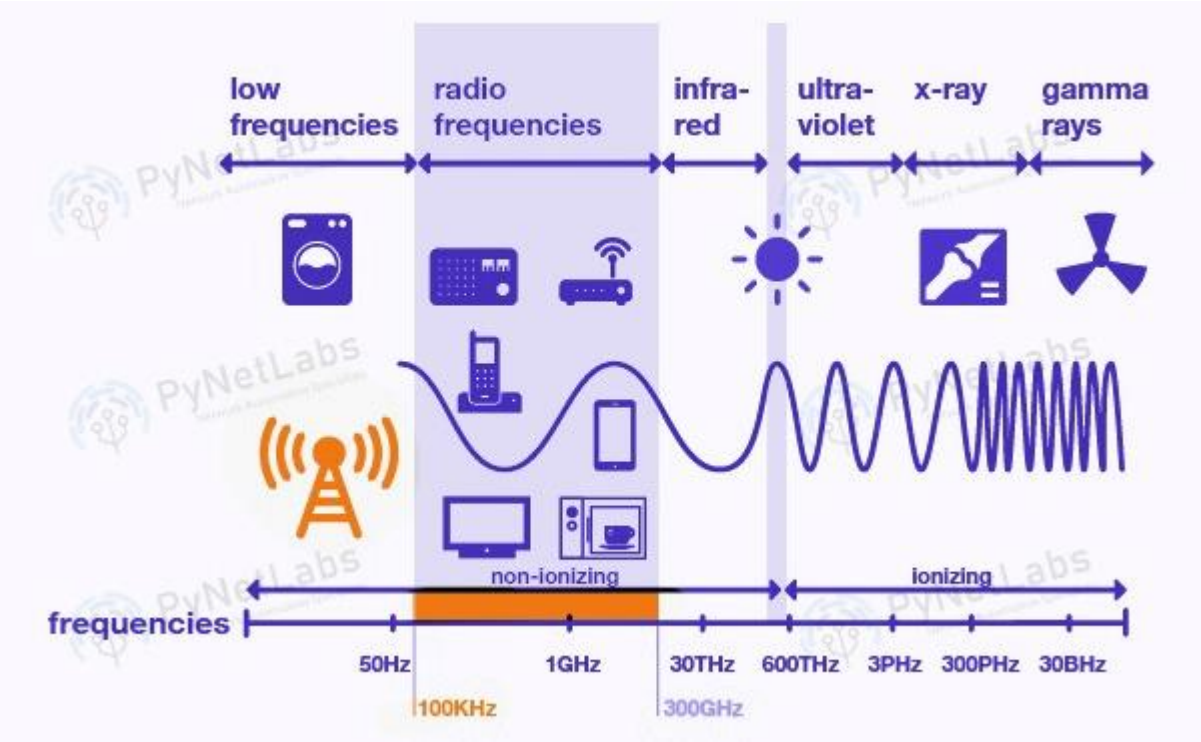
WLANs are utilized in different circumstances and serve their purpose.

Networking and internet services are seen as essential in modern business computing. There is a growing trend of LAN users transitioning towards mobile usage. Mobile users necessitate network connectivity irrespective of location as they seek simultaneous access to the network. Wireless LANs allow users to access shared information without the need for physical connections to their systems, thereby eliminating the need for network managers to install cables and other equipment to set up networks.

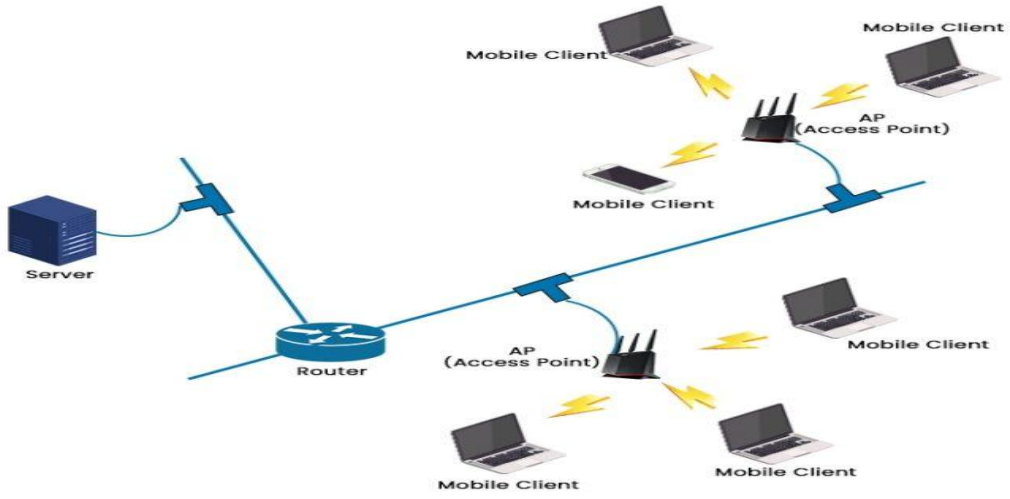
The significance of mobile connectivity is often overlooked; however, it becomes especially critical when one is faced with urgent needs but lacks access to a WLAN.

How Does Wireless Local Area Network Work?

Understanding the functioning of WLAN is straightforward. The operational principles of LAN networking are nearly identical. The only difference is that WLAN allows the connection of devices to a network without the need for a physical cable.



Wireless Local Area Network (WLAN) employs radio frequency waves to help with the transmission and reception of data among various devices, such as a wireless router and a laptop.



Wireless LAN

Radio waves are commonly known as radio carriers due to their primary role of transmitting energy to a distant receiver. The radio carrier overlays the transmitted data, thereby allowing its precise retrieval upon reception.

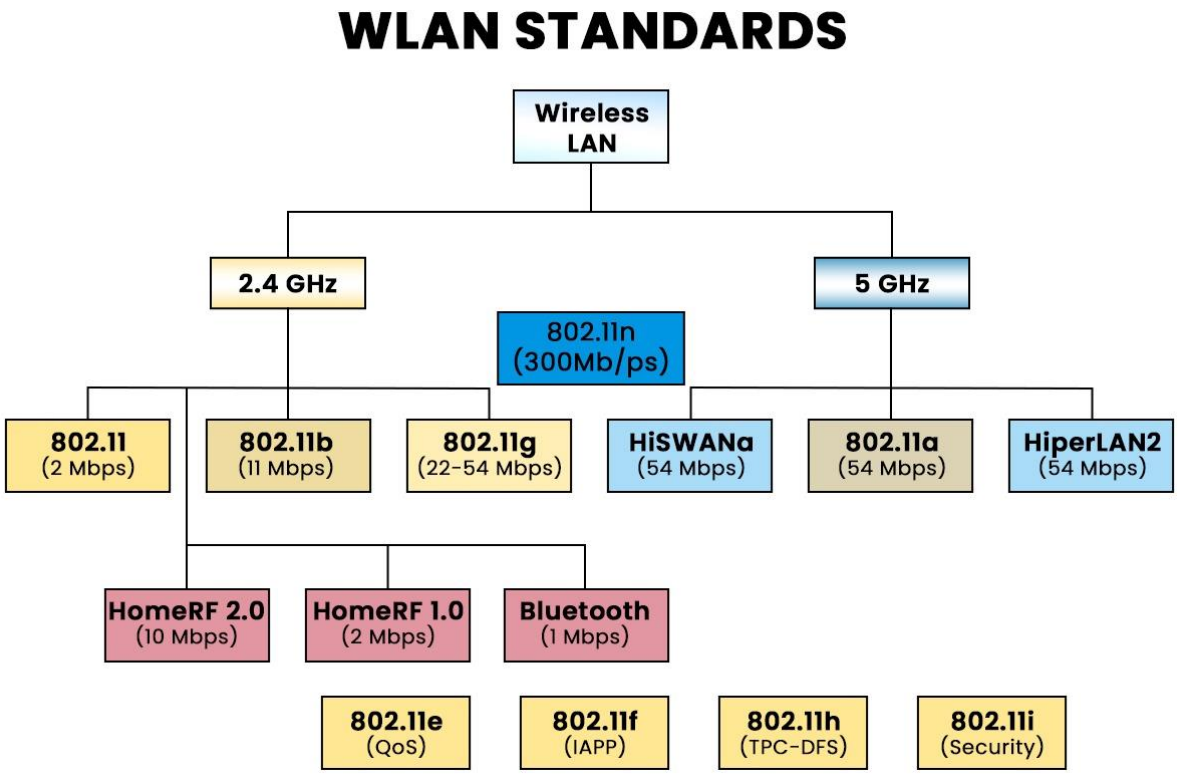
The process is commonly known as modulation. In a wireless local area network setup, a transceiver device, commonly referred to as an access point, establishes a connection to the wired network via standard cabling from a fixed position. The access point functions as an intermediary device that allows the transfer of data between the WLAN and the wired network infrastructure by receiving, buffering, and retransmitting the data.

A single access point can handle a limited number of users and can operate within a distance from under one hundred to multiple hundred feet. Typically, the access point, along with its attached antenna, is installed at an elevated position. However, it may be situated in any feasible location that achieves the desired radio coverage.

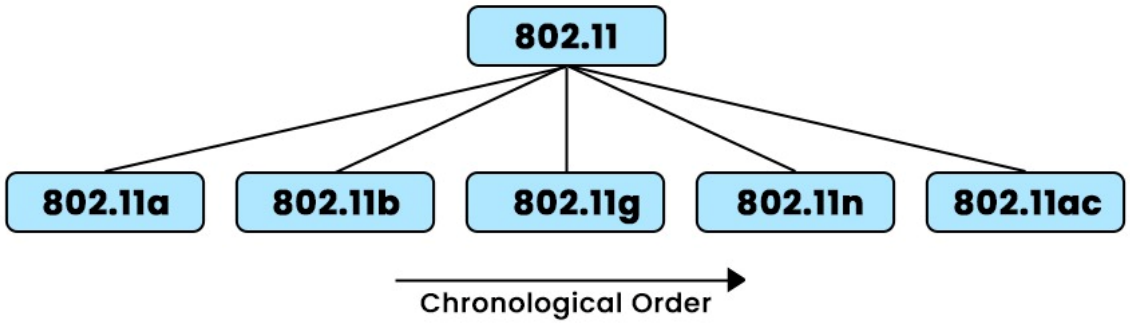
Wireless LAN adapters serve as the medium through which end users gain access to the wireless LAN. These adapters are available in the form of add-on cards for notebook or palmtop computers, as cards for desktop computers, or as integrated components within hand-held computers. WLAN adapters allow a communication interface between the client's network operating system (NOS) and the airwaves through an antenna.

Wireless LAN Standards and Modes

IEEE 802.11 is the standard protocol for wireless local area networks that make it possible to connect securely to high-speed wireless networks while still having mobile access to network infrastructure. Before the advent of this technology, we needed to be connected with cables to the LAN to enjoy the benefits of a fast connection speed while using a network.



Several WLAN standards and modes have been designed throughout time by multiple organizations in the business world. The following diagram illustrates many of the most popular WLAN modes and standards.



802.11 was first developed in 1997, and after that various updates are developed as per the requirements.

Advantages of Wireless LAN in Computer Networks
Some of the benefits associated with the Wireless LANs are:

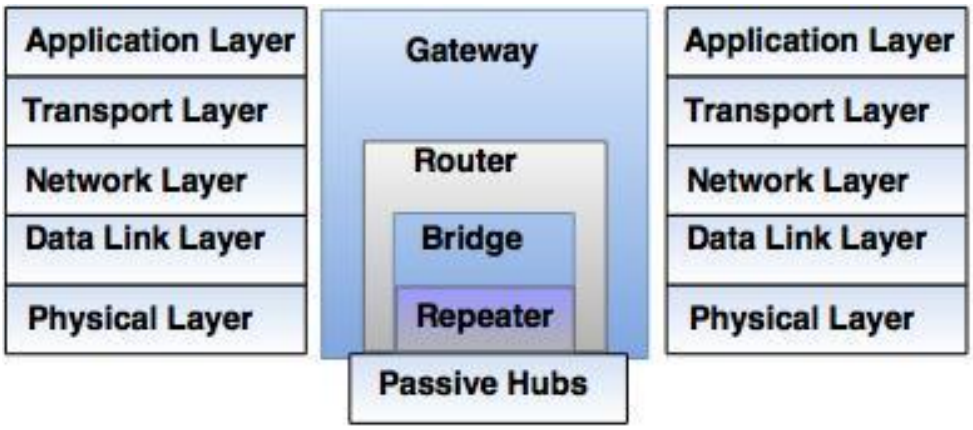
- **Mobility:** WLANs allow users to access network resources and services from anywhere within the coverage area without being restricted by cables or wires. This increases productivity and flexibility for users working from different locations or moving around while staying connected.
- **Scalability:** WLANs can easily accommodate changes in the network's number of devices or users by adding or removing access points as needed. WLANs can also support different types of devices and applications, such as voice, video, and data.
- **Cost:** WLANs can reduce the cost of network installation and maintenance costs by eliminating the need for wiring and cabling. WLANs can also save energy and space by using less power and equipment than wired networks.
- **Security:** Using encryption, authentication, and firewall technologies, WLANs can provide secure network access to authorized users. Using frequency hopping and spread spectrum techniques, WLANs can also protect the network from interference and eavesdropping.

Disadvantages of Wireless LAN
Here are some disadvantages of Wireless LAN -

- **Limited range:** WLAN signals have a limited coverage area compared to wired networks.
- **Interference and congestion:** Wireless networks can experience interference and congestion from other devices and neighboring networks.
- **Security concerns:** WLANs are more susceptible to unauthorized access and data breaches without proper security measures.
- **Signal degradation:** WLAN signals can be affected by distance, physical obstructions, and electromagnetic interference, leading to reduced performance.
- **Reliability and performance issues:** WLANs may experience dropped connections, latency, and slower data transfer speeds.
- **Cost and complexity:** Setting up and maintaining a WLAN can be more expensive and complex compared to wired networks.

Connecting Devices

Connecting devices are divided into five different categories on the basis of layers in which they operate in the network.



Types of Connecting Devices

1. Devices which operate below the physical layer. For example: Passive hub.

2. Devices which operate at the physical layer. For example: Repeater.

3. Devices which operate at the physical and data link layers. For example: Bridge.

4. Devices which operate at the physical layer, data link layer and network layer. For example: Router.

5. Devices which operate at all five layers. For example: Gateway.

1. Hubs

- Several networks need a central location to connect media segments together. These central locations are called as hubs.
- The hub organizes the cables and transmits incoming signals to the other media segments.

The three types of hubs are:

i) Passive hub

- It is a connector, which connects wires coming from the different branches.
- By using passive hub, each computer can receive the signal which is sent from all other computers connected in the hub.

ii) Active Hub

- It is a multiport repeater, which can regenerate the signal.
- It is used to create connections between two or more stations in a physical star topology.

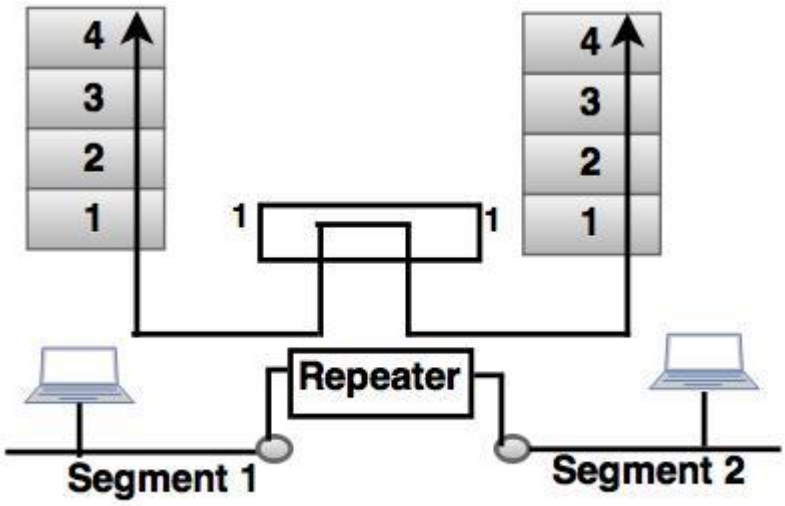
iii) Intelligent Hub

- Intelligent hub contains a program of network management and intelligent path selection.

For example: Switching hub.

2. Repeaters

- Repeater works on physical layer.
- A repeater receives the signal and it regenerates the signal in original bit pattern before the signal gets corrupted.
- It is used to extend the physical distance of LAN. A repeater cannot connect two LANs, but it connects two segments of the same LAN.

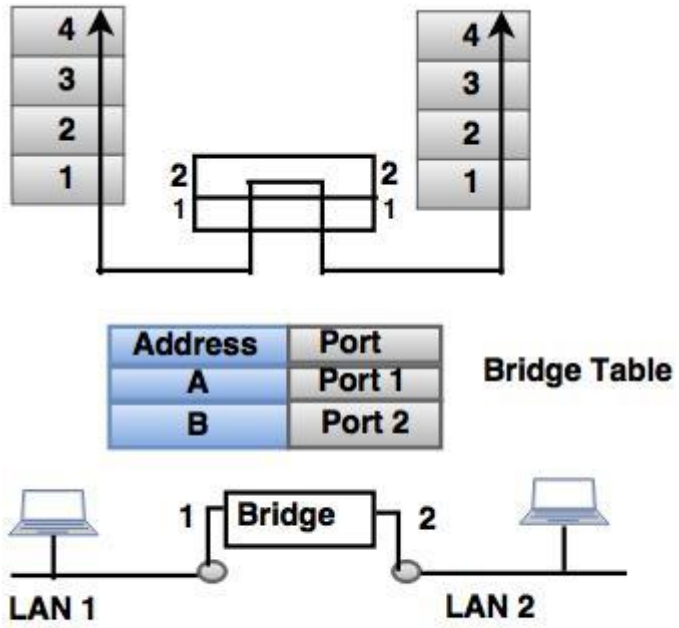


Repeater

3. Bridges

- Bridges operate in physical layer as well as data link layer.
- As a physical layer device, they regenerate the receive signal.
- As a data link layer, the bridge checks the physical (MAC) address (of the source and the destination) contained in the frame.

- The bridge has a filtering feature. It can check the destination address of a frame and decides, if the the frame should be forwarded or drooped.



Bridge connecting Two LAN's

4. Switches

- It supports transmitting, receiving and controlling of traffic with other computers on the network.
- MAC address (48 bit) is hard-coded on the card by the manufacturer. This MAC address is globally unique.
- NIC is specific to a particular type of LAN architecture.
- For example: Fiber optic
- When NIC transmits data on network, it converts data from parallel to serial and then encodes and compresses it. After receiving data, NIC translates the electrical signal into binary that can be read by computer.
- NIC operates at physical layer of OSI model.
- The MAC address can distinguish one NIC from any other NIC.

i) Two- Layer Switch

- The two-layer switch performs at the physical and the data link layer.
- It is a bridge with many ports and design allows faster performs.
- A bridge is used to connect different LANs together.
- The two- layer switch can make a filtering decision bases on the MAC address of the received frame. However, two- layer switch has a buffer which holds the frame for processing.

ii) Three- Layer Switch

- The three-layer switch is a router.
- The switching fabric in a three-layer allows a faster table lookup and forwarding mechanism.

5. Routers

- The router is a three-layer device, which can route the packets based on their logical addresses (host-to-host addressing).
- A router connects the LANs and WANs on the internet.
- Router has a routing table, which is used to make decision on selecting the route.
- The key function of the router is to determine the shortest path to the destination.

6. Gateway

- A gateway is a computer, which operates in all five layers of the internet or seven layers of OSI model.
- Gateway connects two independent networks.
- A gateway accepts a packet formatted for one protocol (for example, TCP/IP) and converts it to a packet formatted to another protocol (for example, Apple Talk) before forwarding it.
- The gateway must adjust the data rate, size and data format.