RGPVNOTES.IN

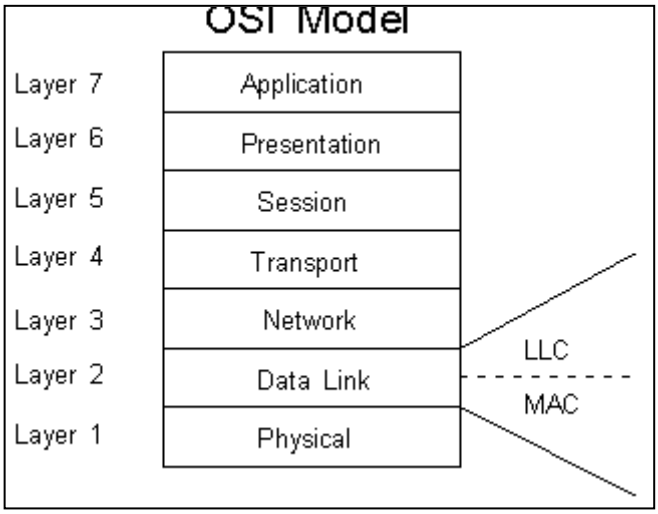
Subject Name: **Computer Network**

Subject Code: **IT-5003**

Semester: **5th**

UNIT III

MAC Sublayer



In the seven-layer OSI model of computer networking, media access control (MAC) data communication protocol is a sublayer of the data link layer (layer 2). The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a media access controller.

The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

MAC Addressing (Media Access Control address)

In a local area network (LAN) or another network, the MAC (Media Access Control) address is your computer's unique hardware number.

In a local area network (LAN) or another network, the MAC (Media Access Control) address is your computer’s unique hardware number. (On an Ethernet LAN, it’s the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

MAC Address

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN. MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

MM: MM: MM: SS: SS: SS MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. In the example, 00: A0: C9:14: C8:29

The prefix 00A0C9 indicates the manufacturer is Intel Corporation.

Why MAC Addresses

Recall that TCP/IP and other mainstream networking architectures generally adopt the OSI model. In this model, network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in /the OSI model). They allow computers to uniquely identify themselves on a network at this relatively

low level.

MAC vs. IP Addressing

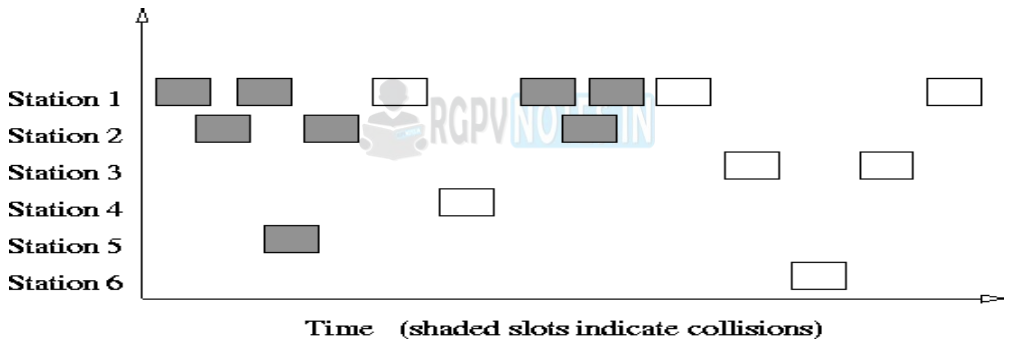
Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device move from one network to another.

IP networks maintain a mapping between the IP address of a device and its MAC address. This mapping is known as the ARP cache or ARP table. ARP, the Address Resolution Protocol, supports the logic for obtaining this mapping and keeping the cache up to date. DHCP also usually relies on MAC addresses to manage the unique assignment of IP addresses to devices.

Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted ALOHA)

Pure Aloha

Pure Aloha is an unspotted, fully-decentralized protocol. It is extremely simple and trivial to implement. The ground rule is - "when you want to talk, just talk!". So, a node which wants to transmit, will go ahead and send the packet on its broadcast channel, with no consideration whatsoever as to anybody else is transmitting or not.



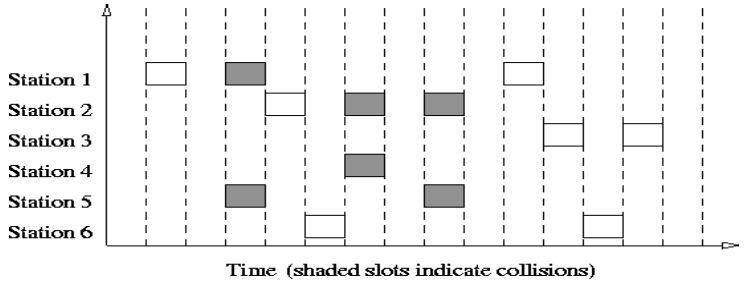
One serious drawback here is that you don't know whether what you are sending has been received properly or not (so as to say, "whether you've been heard and understood?"). To resolve this, in Pure Aloha, when one node finishes speaking, it expects an acknowledgment in a finite amount of time - otherwise, it simply retransmits the data. This scheme works well for small networks where the load is not high. But in large, load intensive networks where many nodes may want to transmit at the same time, this scheme fails miserably. This led to the development of Slotted Aloha.

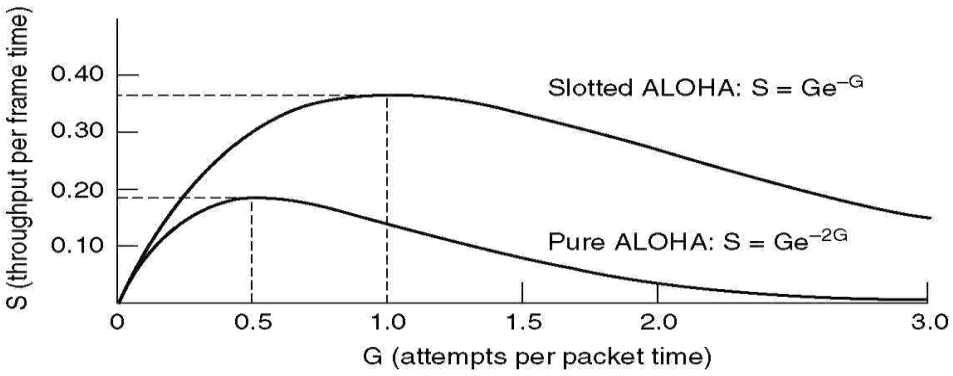
Slotted Aloha

This is quite similar to Pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at demand time, the sender waits for some time. This delay is specified as follows - the timeline is divided into equal slots and then it is required that transmission should take place only at slot boundaries. To be more precise, the slotted-Aloha makes the following assumptions:

- All frames consist of exactly L bits.
- Time is divided into slots of size L/R seconds (i.e., a slot equals the time to transmit one frame).
- Nodes start to transmit frames only at the beginnings of slots.
- The nodes are synchronized so that each node knows when the slots begin.

- If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends.





In this way, the number of collisions that can possibly take place is reduced by a huge margin. And hence, the performance become much better compared to Pure Aloha. collisions may only take place with nodes that are ready to speak at the same time. But nevertheless, this is a substantial reduction.

Carrier Sense Multiple Access Protocols

In both slotted and pure ALOHA, a node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel. A node neither pays attention to whether another node happens to be transmitting when it begins to transmit nor stops transmitting if another node begins to interfere with its transmission. As humans, we have human protocols that allow allows us to not only behave with more civility but also to decrease the amount of time spent "colliding" with each other in conversation and consequently increasing the amount of data we exchange in our conversations. Specifically, there are two important rules for polite human conversation:

1. Listen before speaking: If someone else is speaking, wait until they are done. In the networking world, this is termed carrier sensing - a node listens to the channel before transmitting. If a frame from another node is currently being transmitted over the channel, a node then waits ("backs off") a random amount of time and then again senses the channel. If the channel is sensed to be idle, the node then begins frame transmission. Otherwise, the node waits another random amount of time and repeats this process.
2. If someone else begins talking at the same time, stop talking. In the networking world, this is termed collision detection - a transmitting node listens to the channel while it is transmitting. If it detects that another node is transmitting an interfering frame, it stops transmitting and uses some protocol to determine when it should next attempt to transmit.

It is evident that the end-to-end channel propagation delay of a broadcast channel - the time it takes for a signal to propagate from one of the channels to another - will play a crucial role in determining its performance. The longer this propagation delay, the larger the chance that a carrier-sensing node is not yet able to sense a transmission that has already begun at another node in the network.

CSMA- Carrier Sense Multiple Access

This is the simplest version CSMA protocol as described above. It does not specify any collision detection or handling. So, collisions might and WILL occur and clearly, then, this is not a very good protocol for large, load intensive networks.

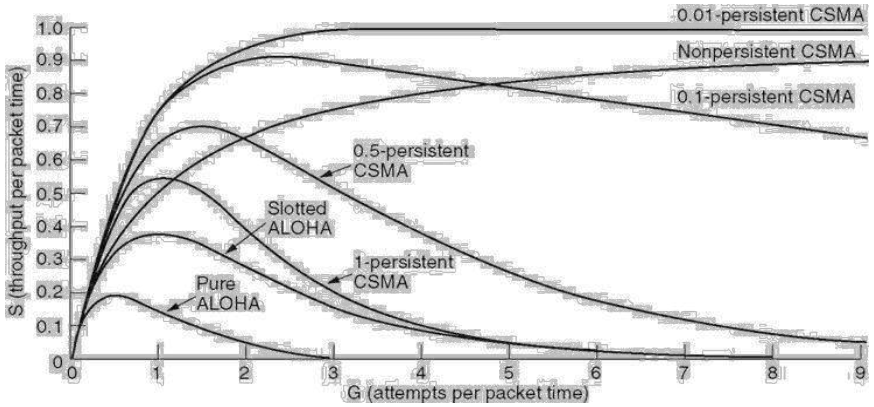
So, we need an improvement over CSMA - this led to the development of CSMA/CD.

CSMA/CD- CSMA with Collision Detection

In this protocol, while transmitting the data, the sender simultaneously tries to receive it. So, as soon as it detects a collision 6hy (it doesn't receive its own data) it stops transmitting. Thereafter, the node waits for some time interval before attempting to transmit again. Simply put, "listen while you talk". But, how long should one wait for the carrier to be freed? There are three schemes to handle this:

1. 1-Persistent: In this scheme, transmission proceeds immediately if the carrier is idle. However, if the carrier is busy, then sender continues to sense the carrier until it becomes idle. The main problem here is that, if more than one transmitters are ready to send, a collision is GUARANTEED!!
2. Non-Persistent: In this scheme, the broadcast channel is not monitored continuously. The sender polls it at random time intervals and transmits whenever the carrier is idle. This decreases the probability of collisions. But, it is not efficient in a low load situation, where a number of collisions are anyway small. The problems it entails are:
   - If back-off time is too long, the idle time of carrier is wasted in some sense
   - It may result in long access delays
3. p-Persistent: Even if a sender finds the carrier to be idle, it uses a probabilistic distribution to determine whether to transmit or not. Put simply, "toss a coin to decide". If the carrier is idle, then transmission takes place with a probability p and the sender waits with a probability 1-p. This scheme is a good tradeoff between the Non-persistent and 1-persistent schemes. So, for low load situations, p is high (example: 1-persistent); and for high load situations, p may be lower. Clearly, the value of p plays an important role in determining the performance of this protocol. Also, the same p is likely to provide different performance at different loads.

CSMA/CD doesn't work in some wireless scenarios called "hidden node" problems. Consider a situation, where there are 3 nodes - A, B and C communicating with each other using a wireless protocol. Moreover, B can communicate with both A and C, but A and C lie outside of each other's range and hence can't communicate directly with each other. Now, suppose both A and C want to communicate with B simultaneously. They both will sense the carrier to be idle and hence will begin transmission, and even if there is a collision, neither A nor C will ever detect it. B, on the other hand, will receive 2 packets at the same time and might not be able to understand either of them. To get around this problem, a better version called CSMA/CA was developed, especially for wireless applications.



Basic Bit Map

This is how the Basic Bit-Map Protocol works.

A Bit-Map protocol

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

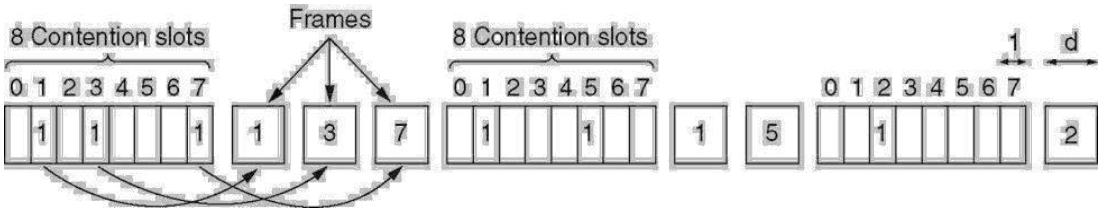


Figure: The basic Bitmap Protocol

- Consider the situation from the point of view of a low-numbered station, such as 0 or 1.
- Typically, when it becomes ready to send, the "current" slot will be somewhere in the middle of the bitmap.
- On average, the station will have to wait for N/2 slots for the current scan to finish and another full N slots for the following scan to run to completion before it may begin transmitting.
- The prospects for high-numbered stations are brighter. Generally, these will only have to wait for half a scan (N/2 bit slots) before starting to transmit. High-numbered stations rarely have to wait for the next scan.
- Since low-numbered stations must wait on average 1.5N slots and high-numbered stations must wait on average 0.5N slots, the mean for all stations is N slots.
- The channel efficiency at low load is easy to compute. The overhead per frame is N bits and the the amount of data is d bits, for an efficiency of d/ (N + d).
- At high load, when all the stations have something to send all the time, the N-bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame, or an efficiency of d/ (d + 1).
- The mean delay for a frame is equal to the sum of the time it queues inside its station, plus an additional N (d + 1)/2 once it gets to the head of its internal queue.

BRAP

Backup Route Aware Routing Program (BRAP) is a protocol that provides interdomain routing. BRAP uses reverse paths and backup paths to ensure fast failure recovery in networking systems.

Binary Count Down

One problem with Basic Bit-Map Protocol is that the overhead is 1 bit per frame per station. We can do better by using binary station addresses.

- A station wanting to use the channel now broadcasts its address as a binary bit string in a serial fashion.
- As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten by a 1, it gives up (meaning some high order station wants to transmit).
- The remaining stations keep sending their addresses on the network until a winner emerges.
- The winning station sends out the frame. The bidding process repeats.

For example, if stations 0010, 0100, 1001, and 1010 are all trying to get the channel, in the first-bit time the four stations transmit 0, 0, 1, and 1, respectively. These are ORed together resulting in a 1. Stations 0010 and 0100 see the 1 and know that a higher-numbered station is competing for the channel, so they give up for the current round. Stations 1001 and 1010 continue. The next bit sent from both stations is 0, both continues. The next bit is 1, so station 1001 gives up. The winner is 1010. This station transmits its frame. Then a new bidding process begins. The channel efficiency is now d/ (d + ln N)

Ethernet 802.3

Ethernet is a widely deployed LAN technology. This technology was invented by Bob Metcalfe and D.R. Boggs in the year 1970. It was standardized in IEEE 802.3 in 1980.

Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data.

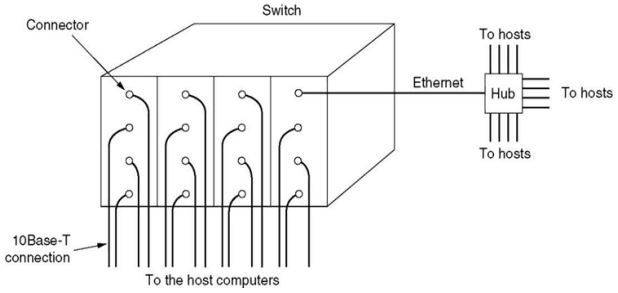
Ethernet connector is, network interface card equipped with 48-bits MAC address. This helps other Ethernet devices to identify and communicate with remote devices in Ethernet.

Traditional Ethernet uses 10BASE-T specifications. The number 10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5 twisted pair cable with RJ-45 connector. Ethernet follows star topology with segment length up to 100 meters. All devices are connected to a hub/switch in a star fashion.

High-Speed LAN: Fast Ethernet, Gigabit Ethernet

Ethernet is one of the widely used local area network (LAN) technology.

Switched Ethernet



- Switched Ethernet gives dedicated 10 Mbps bandwidth on each of its ports.
- On each of the ports, one can connect either a thick/thin segment or a computer.

- In Switched Ethernet, the collision domain is separated.
- The hub is replaced by a switch, which functions as a fast bridge.
- It can recognize the destination address of the received frame and can forward the frame to the port
- to which the destination station is connected.
- The other ports are not involved in the transmission process.
- The switch can receive another frame from another station at the same time and can route this frame to its own destination.
- In this case, both the physical and logical topologies are a star.
- The throughput can be further increased on switched Ethernet by using the full-duplex technique, which uses separate wire pairs for transmitting and receiving.
- Thus, a station can transmit and receive simultaneously, effectively doubling the throughput to 20 Mbps on each port.

Fast Ethernet

- The 802.u or the fast Ethernet, as it is commonly known, was approved by the IEEE 802 committee.
- The fast Ethernet uses the same frame format, same CSMA/CD protocol and same interface as the 802.3, but uses a data transfer rate of 100 Mbps instead of 10 Mbps.
- However, fast Ethernet is based entirely on 10-Base-T, because of its advantages (Although technically 10-BASE-5 or 10-BASE-2 can be used with shorter segment length).
- IEEE has designed two categories of Fast Ethernet: 100Base-X and 100Base-T4.
- 100Base-X uses two-wire interface between a hub and a station while 100Base-T4 uses four-wire interface.
- 100-Base-X itself is divided into two: 100Base-TX and 100base-FX

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Gigabyte Ethernet

- The technology is based on fiber optic cable. Multi-mode fiber can transmit at gigabit rate to at least 580 meters and with single-mode runs exceeding 3 km.
- Fiber optic cabling is costly. To reduce the cost of cabling, the 802.3z working group also proposed the use of twisted pair or cable or coaxial cable for distances up to 30 meters.
- At gigabit speed, two stations 200 meters apart will not detect a collision, when both simultaneously send 64-byte frames.
- This inability to detect collision leads to network instability.
- A mechanism known as *carrier extension* has been proposed for frames shorter than 512 bytes.
- The number of repeater hops is also restricted to only one in place of two for 100 Base-T.

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Token Bus 802.4

In token bus Computer network station must have possession of a token before it can transmit on the computer network. The IEEE 802.4 Committee has defined token bus standards as broadband computer networks, as opposed to Ethernet's baseband transmission technique. Physically, the token bus is a linear or tree-shape cable to which the stations are attached

The topology of the computer network can include groups of workstations connected by long trunk cables. Logically, the stations are organized into a ring. These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance. IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology. The broadba nd characteristics of the 802.4 standard support transmission over several different channels simultaneously.

When the logical ring is initialized, the highest numbered station may send the first frame. The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring. The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.

In such a case, there is no collision as only one station possesses a token at any given time. In token bus, each station receives each frame; the station whose address is specified in the frame processes it and the other stations discard the frame.

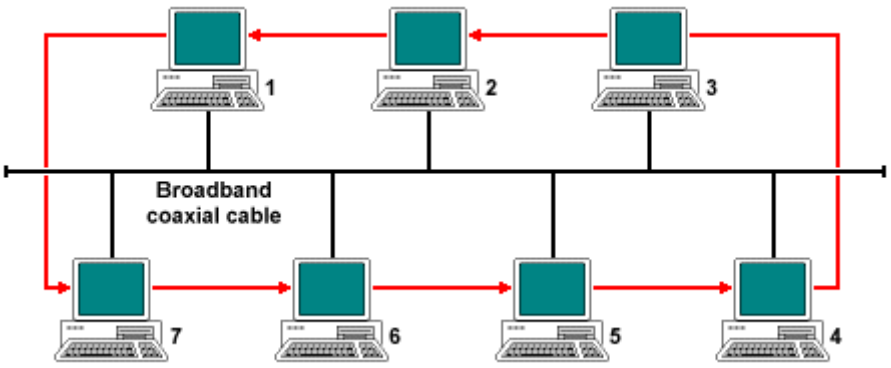


Figure:- Token Bus

MAC Sublayer Function

• When the ring is initialized, stations are inserted into it in order of station address, from highest to lowest.

• Token passing is done from high to low address.

• Whenever a station acquires the token, it can transmit frames for a specific amount of time.

• If a station has no data, it passes the token immediately upon receiving it.

• The token bus defines four priority classes, 0, 2, 4, and 6 for traffic, with 0 the lowest and 6 the highest.

• Each station is internally divided into four substations, one at each priority level *i.e.* 0,2,4 and 6.

• As input comes in to the MAC sublayer from above, the data are checked for priority and routed to one of

the four substations.

• Thus, each station maintains its own queue of frames to be transmitted.

• When a token comes into the station over the cable, it is passed internally to the priority 6 substation, which can begin transmitting its frames, if it has any.

• When it is done or when its time expires, the token is passed to the priority 4 substation, which can then transmit frames until its timer expires. After this the token is then passed internally to priority 2 substation.

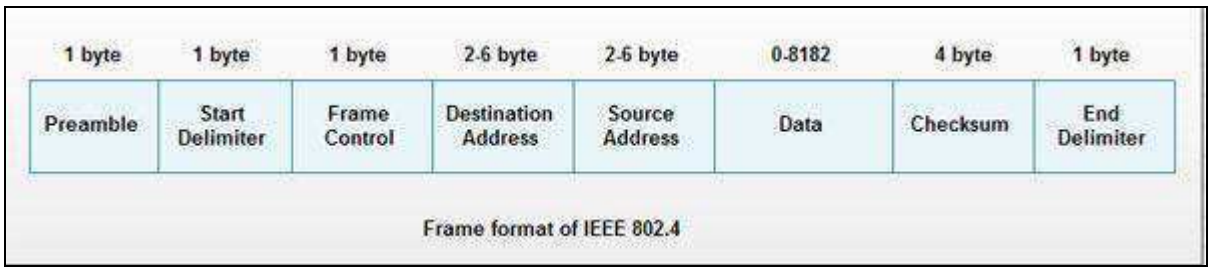
• This process continues until either the priority 0 substation has sent all its frames or its time expires.

• After this the token is passed to the next station in the ring.

Frame format of Token Bus

The various fields present in the frame format are

1. **Preamble**: This. Field is at least 1-byte long. It is used for bit synchronization.



Frame format of IEEE 802.4

2. **Start Delimiter**: This one-byte field marks the beginning of frame.

3. **Frame Control:** This one-byte field specifies the type of frame. It distinguishes data frame from control frames. For data frames, it carries frame's priority. For control frames, it specifies the frame type. The control frame types include. token passing and various ring maintenance frames, including the mechanism for letting new station enter the ring, the mechanism for allowing stations to leave the ring.

4. **Destination address**: It specifies 2 to 6 bytes destination address.

5. **Source address**: It specifies 2 to 6 bytes source address.

6. **Data**: This field may be up to 8182 bytes long when 2 bytes addresses are used & upto 8174 bytes long when 6 bytes address is used.

7. **Checksum**: This 4-byte field detects transmission errors.

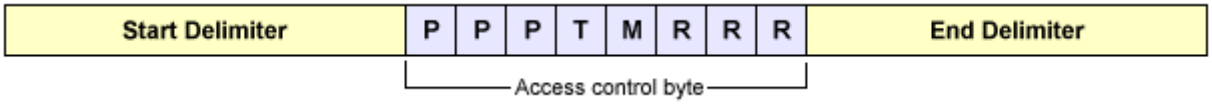
8. **End Delimiter**: This one-byte field marks the end of frame.

Token Ring 802.5

Token Ring was developed by IBM in the 1970s and is described in the IEEE 802.5 specification. It is no longer widely used in LANs. Token passing is the method of medium access, with only one token allowed to exist on the network at any one time. Network devices must acquire the token to transmit data, and may only transmit a single frame before releasing the token to the next station on the ring. When a station has data to transmit, it acquires the token at the earliest opportunity, marks it as busy, and attaches the data and control information to the token to create a data frame, which is then transmitted to the next station on the ring. The frame will be relayed around the ring until it reaches the destination station, which reads the data, marks the frame as having been read, and sends it on around the ring. When the sender receives the acknowledged data frame, it generates a new token, marks it as being available for use, and sends it to the next station. In this way, each of the other stations on the ring will get an opportunity to transmit data (even if they don't have any data to transmit!).

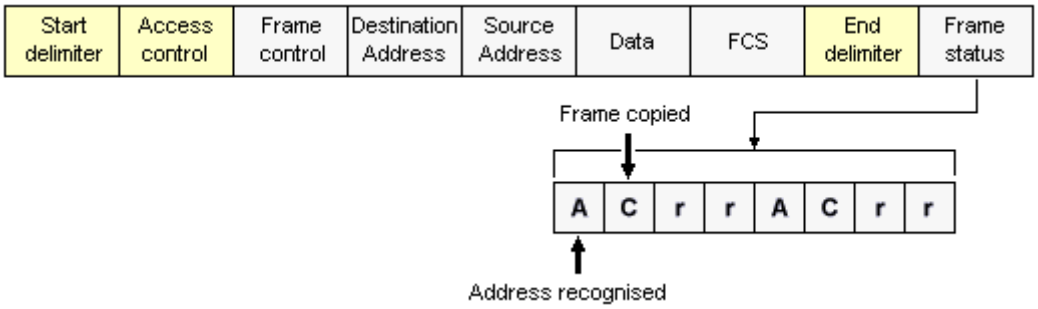
Token Ring networks provide a priority system that allows administrators to designate specific stations as having a higher priority than others, allowing those stations to use the network more frequently by setting the priority level of the token so that only stations with the same priority or higher can use the token (or reserve the token for future use). Stations that raise a token's priority must reinstate the priority level previously in force once they have used the token. In a Token Ring network, one station is arbitrarily selected to be the *active monitor*. The active monitor acts as a source of timing information for other stations, and performs various maintenance functions, such as generating a new token as and when required, or preventing rogue data frames from endlessly circulating around the ring. All of the stations on the ring have a role to play in managing the network, however. Any station that detects a serious problem will generate a *beacon frame* that alerts other stations to the fault condition, prompting them to carry out diagnostic activities and attempt to re-configure the network.

Two basic frame types are used - tokens, and data/command frames. The token is three bytes long and consists of a *start delimiter*, an *access control byte*, and an *end delimiter*. The format of the token is shown below.



The Token Ring token

A data/command frame has the same fields as the token, plus several additional fields. The format of the data/command frame is shown below.



The Token Ring frame format

- ***Start delimiter*** - alerts each station of the arrival of a token or frame.
- ***Access control byte*** - contains the *priority field*, the *reservation field*, the *token bit* and a *monitor bit*.
- ***Frame control byte*** - indicates whether the frame contains data or control information. In a control frame, this byte specifies the type of control information carried.
- ***Destination and source addresses*** - two six-byte fields that identify the destination and source station MAC addresses.
- ***Data*** - the maximum length is limited by the ring *token holding time*, which defines the maximum time a station can hold the token
- ***Frame check sequence (FCS)*** - filled by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- ***End delimiter*** - signals the end of the token or frame, and contains bits that may be used to indicate

a damaged frame, and to identify the last frame in a logical sequence.

- ***Frame status*** - a one-byte field that terminates a frame, and includes the one-bit *address-recognized* and *frame-copied* fields. These one-bit fields, if set, provide confirmation that the frame has been delivered to the source address and the data read. Both fields are duplicated within the frame status byte.

FDDI

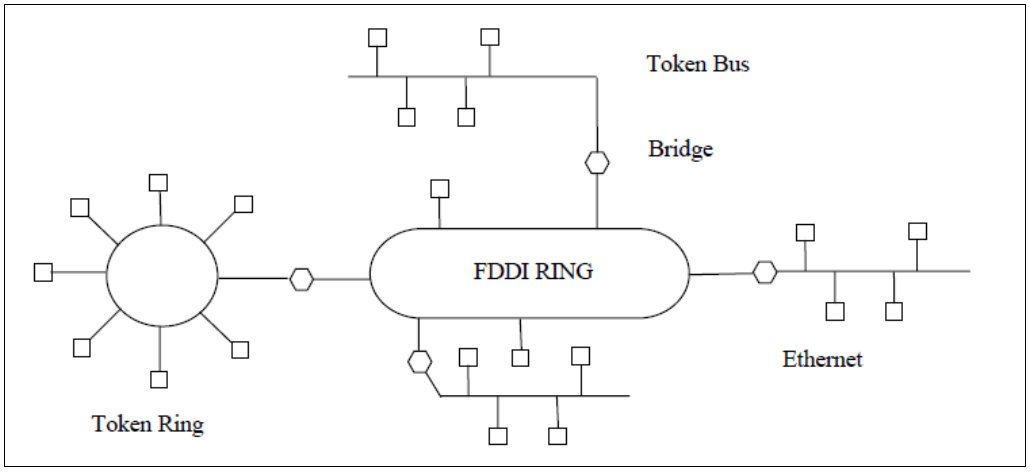
Fiber distributed data interface (FDDI) is a high-performance fiber optic token ring LAN running at 100 Mbps over distances up to 200 km with up to 1000 stations connected. FDDI is used as backbone to connect copper LANs as shown in the figure.

FDDI uses a multimode fiber because the cost of single mode fiber is not justified for networks running at only 100 Mbps. It also uses LEDs instead of Lasers not only because of the lower cost but also because FDDI may sometimes be used to connect directly to user workstations, and safety against exposure to LASER radiation is difficult to maintain in that case. The minimum BER required to be maintained is 1 in 2.5 x 1010.

The FDDI cabling consists of two fiber rings, one transmitting clockwise and the other transmitting counterclockwise. If either one breaks the other act as backup. If both the rings break at the same points, the two rings can be joined to form a new approximately twice as long. This new ring is formed by relays at the two nodes adjoining the broken link.

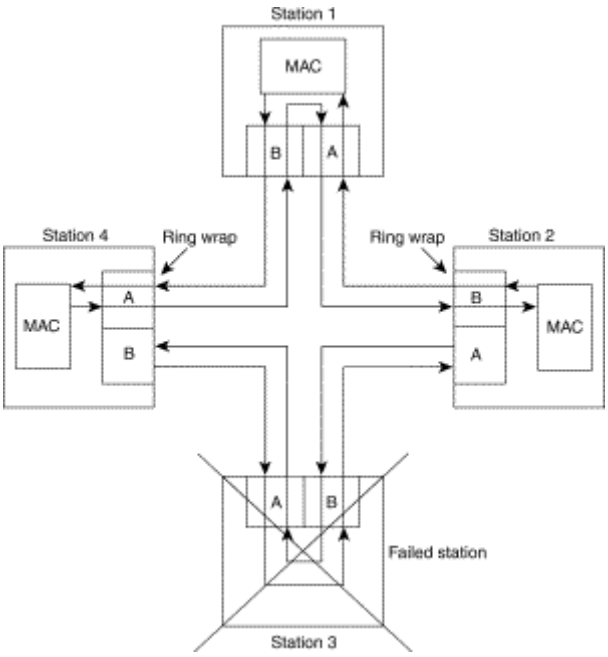
FDDI defines two classes of stations A and B. Class A stations connect to both rings. The cheaper class B stations only connect to one of the rings. Depending on how important fault tolerance is, an installation can choose class A or class B stations.

The physical layer in FDDI uses 4 out of 5 encoding scheme i.e each group of 4 MAC symbols are encoded as a group of 5 bits on the medium. Sixteen of the 32 combinations are for data, 3 are for delimiters, 2 are for control, 3 are for hardware signaling, and 8 are unused. This scheme saves bandwidth but the self-clocking property available with Manchester coding is lost. To compensate a long preamble is used to synchronize the receiver to the sender's clock. The basic FDDI protocols are modeled on the 802.5 protocols. The station must first capture a token, transmit a frame and remove it when it comes around. In FDDI the time spent in waiting for a frame to circumnavigate is reduced by allowing the station to put a new token back onto the ring as soon as it has finished transmitting its frames. In a large ring, several frames may be on the ring at the same time.

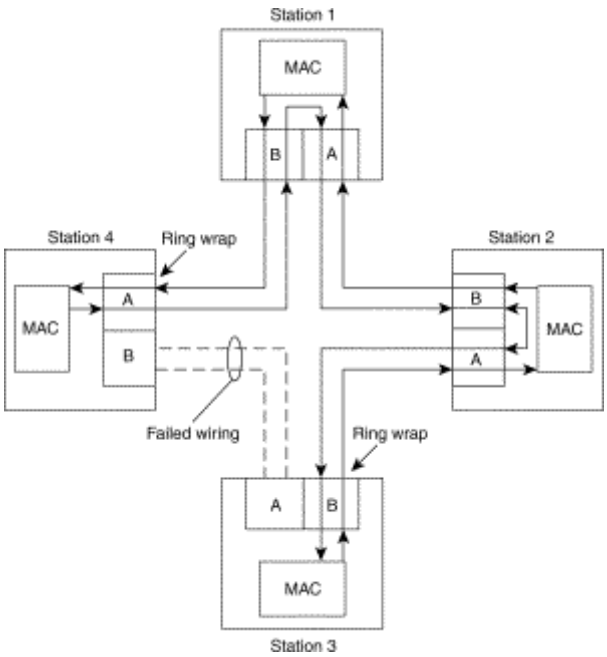


FDDI's four specifications are the Media Access Control (MAC), Physical-Layer Protocol (PHY), Physical-Medium Dependent (PMD), and Station Management (SMT). The MAC specification defines how the medium is accessed, including frame format, token handling, addressing, algorithms for calculating cyclic redundancy check (CRC) value, and error-recovery mechanisms. The PHY specification defines data encoding/decoding procedures, clocking requirements, and framing, among other functions. The PMD specification defines the characteristics of the transmission medium, including fiber-optic links, power levels, bit-error rates, optical components, and connectors. The SMT specification defines FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and statistics collection.

A ring recovers from a station failure by wrapping.



A ring also wraps to withstand a cable failure.



FDDI Frame Format (the FDDI frame is similar to that of a Token Ring frame)

Preamble---A unique sequence that prepares each station for an upcoming frame.

Start Delimiter---Indicates the beginning of a frame by employing a signaling pattern that differentiates it from the rest of the frame.

Frame Control---Indicates the size of the address fields and whether the frame contains asynchronous or synchronous data, among other control information.

Destination Address---Contains a unicast (singular), multicast (group), or broadcast (every station) address. As with Ethernet and Token Ring addresses, FDDI destination addresses are 6 bytes long.

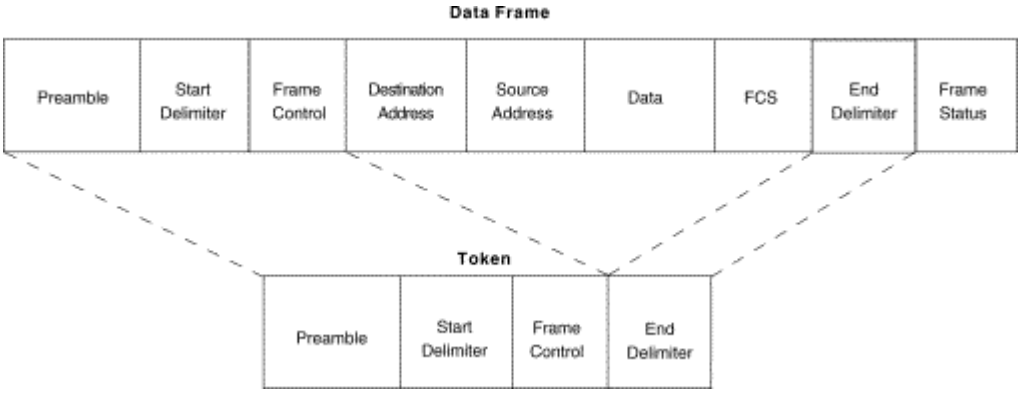
Source Address---Identifies the single station that sent the frame. As with Ethernet and Token Ring addresses, FDDI source addresses are 6 bytes long.

Data---Contains either information destined for an upper-layer protocol or control information.

Frame Check Sequence (FCS)---Filed by the source station with a calculated cyclic redundancy check value dependent on frame contents (as with Token Ring and Ethernet). The destination address recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.

End Delimiter---Contains unique symbols, which cannot be data symbols, that indicate the end of the frame.

Frame Status---Allows the source station to determine whether an error occurred and whether the frame was recognized and copied by a receiving station.



Comparison Between Wired and Wireless LAN

Specifications	Wired network	Wireless network
Speed of operation	Higher	lower compare to wired networks, But advanced wireless technologies such as LTE, LTE-A and WLAN-11ad will make it possible to achieve speed par equivalent to wired network
System Bandwidth	High	Low, as Frequency Spectrum is very scares resource
Cost	Less as cables are not expensive	More as wireless subscriber stations, wireless routers, wireless access points and adapters are expensive

Installation	Wired network installation is cumbersome and it requires more time	Wireless network installation is easy and it requires less time
Mobility	Limited, as it operates in the area covered by connected systems with the wired network	Not limited, as it operates in the entire wireless network coverage
Transmission medium	copper wires, optical fiber cables, ethernet	EM waves or radio waves or infrared
Network coverage extension	requires hubs and switches for network coverage limit extension	More area is covered by wireless base stations which are connected to one another.
Applications	LAN (Ethernet), MAN	WLAN, WPAN(Zigbee, bluetooth), Infrared, Cellular(GSM,CDMA, LTE)
Channel Interference and signal power loss	Interference is less as one wired network will not affect the other	Interference is higher due to obstacles between wireless transmitter and receiver e.g. weather conditions, reflection from walls, etc.
QoS (Quality of Service)	Better	Poor due to high value of jitter and delay in connection setup
Reliability	High compare to wireless counterpart, as manufactured cables have higher performance due to existence of wired technology since years.	Reasonably high, This is due to failure of router will affect the entire network.

WIMAX

WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way.

Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.

WiMAX is derived from Acronym for Worldwide Interoperability for Microwave Access.

Based on Wireless MAN technology.

A wireless technology optimized for the delivery of IP centric services over a wide area.

A scalable wireless platform for constructing alternative and complementary broadband networks.

A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard.

The IEEE 802.16 Working Group develops standards that address two types of usage models –

- A fixed usage model (IEEE 802.16-2004).
- A portable usage model (IEEE 802.16e).

IEEE 802.16a

WiMAX is such an easy term that people tend to use it for the 802.16 standards and technology themselves, although strictly it applies only to systems that meet specific conformance criteria laid down by the WiMAX Forum.

The 802.16a standard for 2-11 GHz is a wireless metropolitan area network (MAN) technology that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.

It can be used to connect 802.11 hot spots to the Internet, provide campus connectivity, and provide a wireless alternative to cable and DSL for last mile broadband access.

WiMax Speed and Range

WiMAX is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the particular technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data.

WiMax developed to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly populated areas. It can also be used to connect WLAN hotspots to the Internet. WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3-km cell coverage area.

Why WiMax ?

- WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, WiFi, and cellular backhaul, providing last-100 meter access from fibre to the curb and giving service providers another cost-effective option for supporting broadband services.

- WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high-value multimedia services.

- WiMAX can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types.

- WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads,

ensuring that subscribers obtain the performance they expect for all types of communications.

- WiMAX, which is an IP-based wireless broadband technology, can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks allowing it to become part of a seamless anytime, anywhere broadband access solution.

- Ultimately, WiMAX is intended to serve as the next step in the evolution of 3G mobile phones, via a potential combination of WiMAX and CDMA standards called 4G.

Range

Wi-Fi typically provides local network access for a few hundred feet with the speed of up to 54 Mbps, a single WiMAX antenna is expected to have a range of up to 40 miles with the speed of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks.

Scalability

Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE device. Fixed channel sizes (20MHz).

WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipment (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.

Bit rate

Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel.

WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.

Quality of Service

Wi-Fi does not guarantee any QoS but WiMax will provide your several levels of QoS.

As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. Wi-Fi does not provide ubiquitous broadband while WiMAX does.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in