RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Computer Networks**

Subject Code: **CS-602**

Semester: **6th**

Department of Computer Science and Engineering
CS602 Computer Networks
Subject Notes: UNIT-III

***Syllabus*: MAC Sub layer: MAC Addressing, Binary Exponential Back-off (BEB) Algorithm, Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted-ALOHA), for Local-Area Networks (CSMA, CSMA/CD, CSMA/CA), Collision Free Protocols: Basic Bit Map, BRAP, Binary Count Down, MLMA Limited Contention Protocols: Adaptive Tree Walk, Performance Measuring Metrics. IEEE Standards 802 series & their variant.**

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.

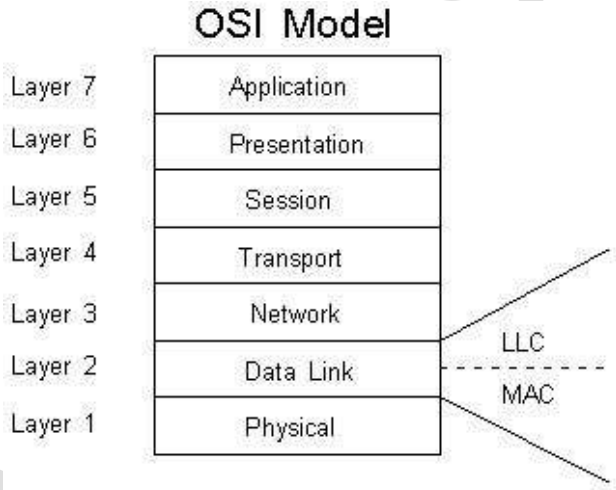


Fig.3.1 MAC Sub Layer

MAC Addressing (Media Access Control address)

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

What Is a 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. 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 moves 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.

Link MAC Address: https://www.youtube.com/watch?v=W52Wt1LDweQ

Binary Exponential Back-off (BEB) Algorithm
In a variety of computer networks, binary exponential back off or truncated binary exponential back off refers to an algorithm used to space out repeated retransmissions of the same block of data, often as part of network congestion avoidance.
Examples are the retransmission of frames in carrier sense multiple access with collision avoidance (CSMA/CA) and carrier sense multiple access with collision detection(CSMA/CD) networks, where this algorithm is part of the channel access method used to send data on these networks. In Ethernet networks, the algorithm is commonly used to schedule retransmissions after collisions. The retransmission is delayed by an amount of time derived from the slot time and the number of attempts to retransmit.
After c collisions, a random number of slot times between 0 and 2c - 1 is chosen. For the first collision, each sender will wait 0 or 1 slot times. After the second collision, the senders will wait anywhere from 0 to 3 slot times (inclusive). After the third collision, the senders will wait anywhere from 0 to 7 slot times (inclusive), and so forth. As the number of retransmission attempts increases, the number of possibilities for delay increases exponentially.

Link: https://www.youtube.com/watch?v=WeGNeUHYv5g

Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted ALOHA)
ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. The original system used for ground-based radio broadcasting, but the system has been implemented in satellite communication systems.
A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. A scientest developed a protocol that would increase the capacity of aloha two-fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different versions

Types of ALOHA:

(i) Pure ALOHA

(ii) Slotted ALOHA

(i) Pure ALOHA

- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore, pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

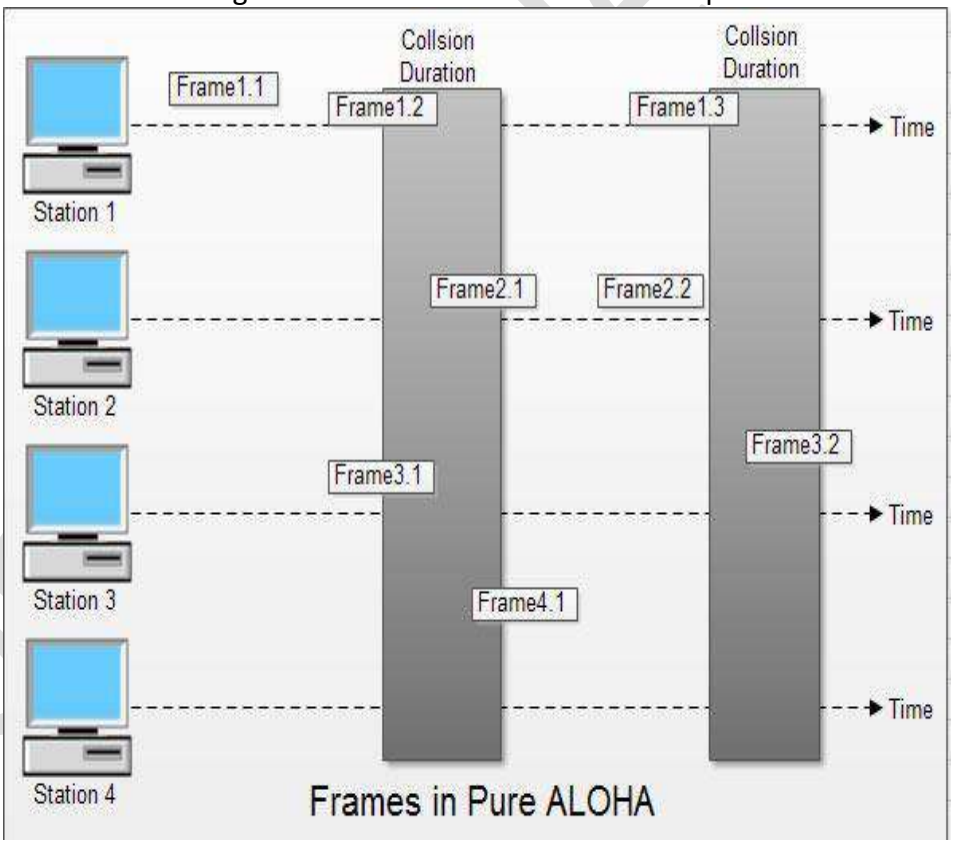


Fig 3.2 Pure ALOHA

(ii) Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.

- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

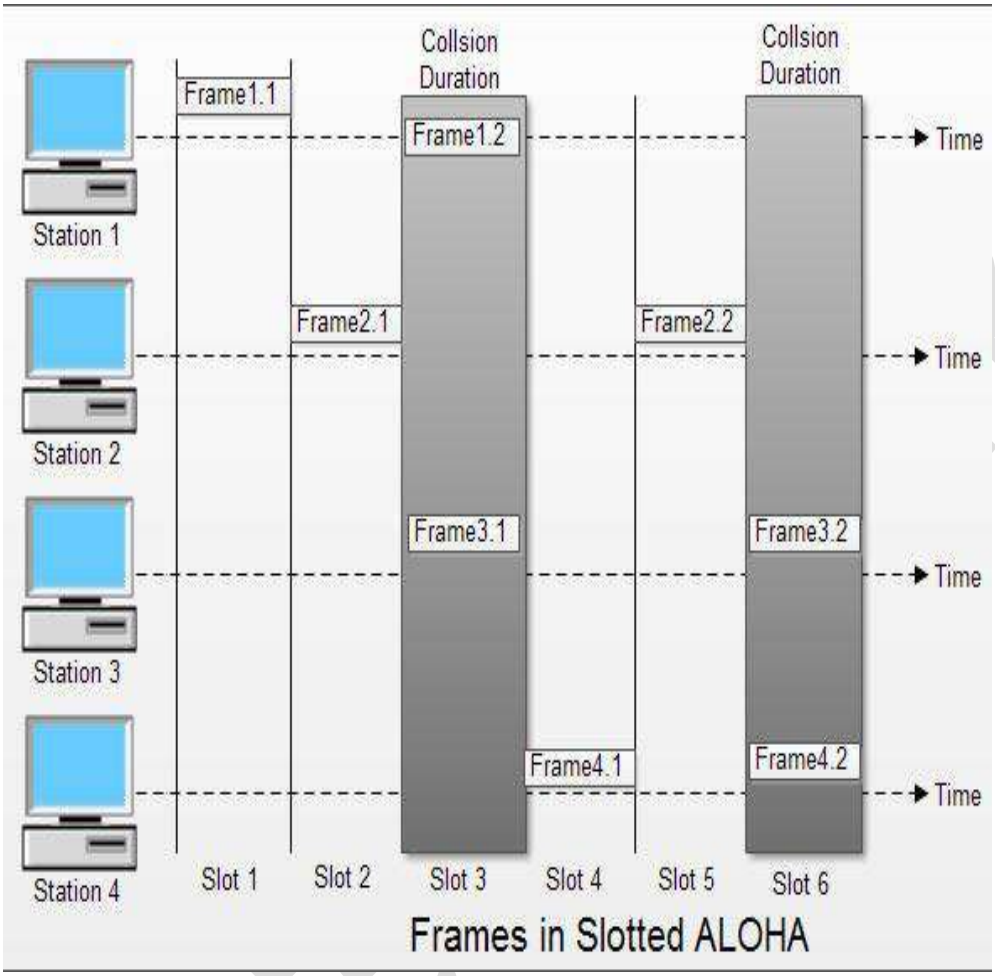


Fig 3.3 Slotted ALOHA

Link ALOHA: https://www.youtube.com/watch?v=c39k2clZU74

For Local-Area Networks (CSMA, CSMA/CD, CSMA/CA)

Carrier sense multiple access (CSMA) is a probabilistic media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.

Carrier sense means that a transmitter uses feedback from a receiver to determine whether another transmission is in progress before initiating a transmission. That is, it tries to detect the presence of a carrier wave from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk".

Multiple access means that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations connected to the medium.

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

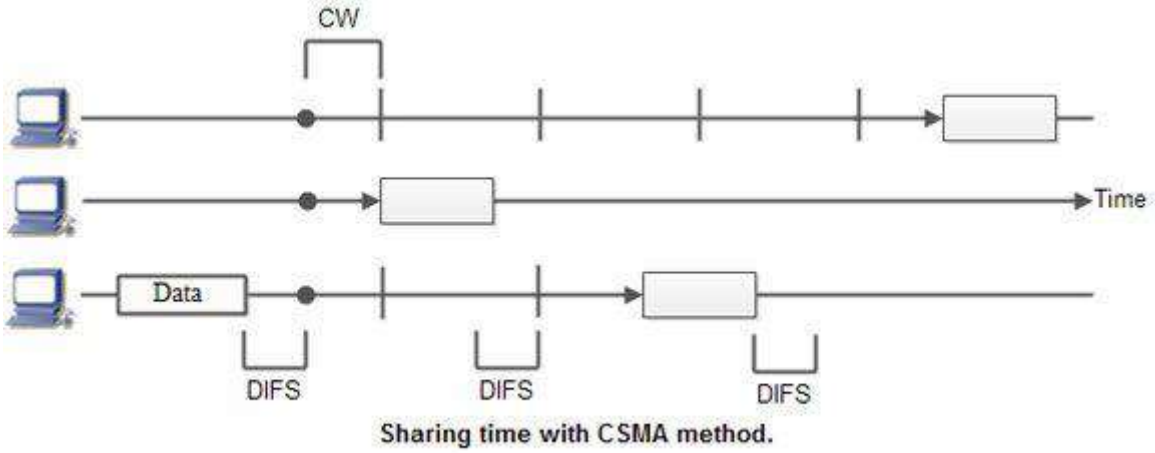


Fig 3.4 CSMA

There Are Three Different Type of CSMA Protocols

(I) 1-persistent CSMA
(ii) Non- Persistent CSMA
(iii) p-persistent CSMA

(i) 1-persistent CSMA

- In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called 1-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start allover again.

Drawback of I-persistent

The propagation delay time greatly affects this protocol. Let us suppose, just after the station 1 begins its transmission, station 2 also became ready to send its data and senses the channel. If the station 1 signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.

Even if propagation delay time is zero, collision will still occur. If two stations became .ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.

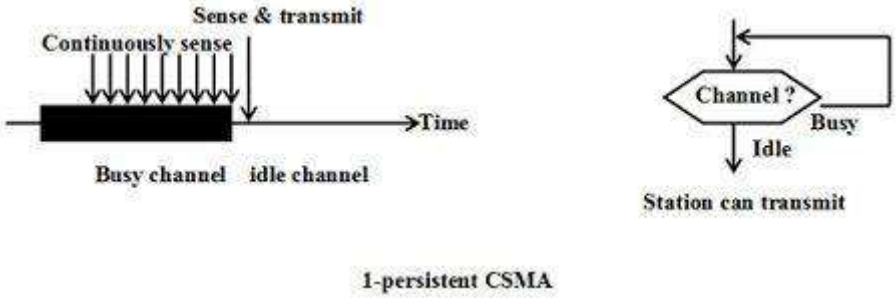


Fig 3.5 1-persistent CSMA

(ii) Non-persistent CSMA

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval oftime.

- After this time, it again checks the status of the channel and if the channel is.free it will transmit.
- A station that has a frame to send senses the channel.
- If the channel is idle, it sends immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantage of non-persistent

- It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

- It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the collision.

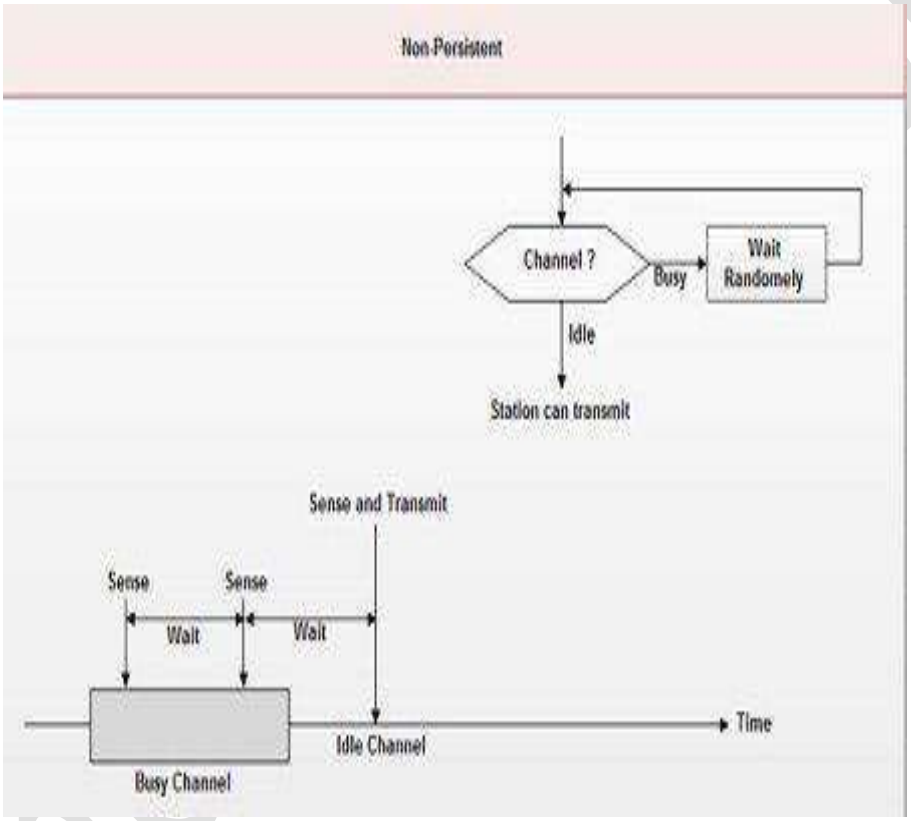


Fig 3.6 Non-persistent CSMA

(iii) p-persistent CSMA

- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- Whenever a station becomes ready to send, it senses the channel.
- If channel is busy, station waits until next slot.
- If channel is idle, it transmits with a probability p.
- With the probability q=1-p, the station then waits for the beginning of the next time slot.
- If the next slot is also idle, it either transmits or waits again with probabilities p and q.
- This process is repeated till either frame has been transmitted or another station has begun transmitting.

- In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.

Advantage of p-persistent

- It reduces the chance of collision and improves the efficiency of the network.

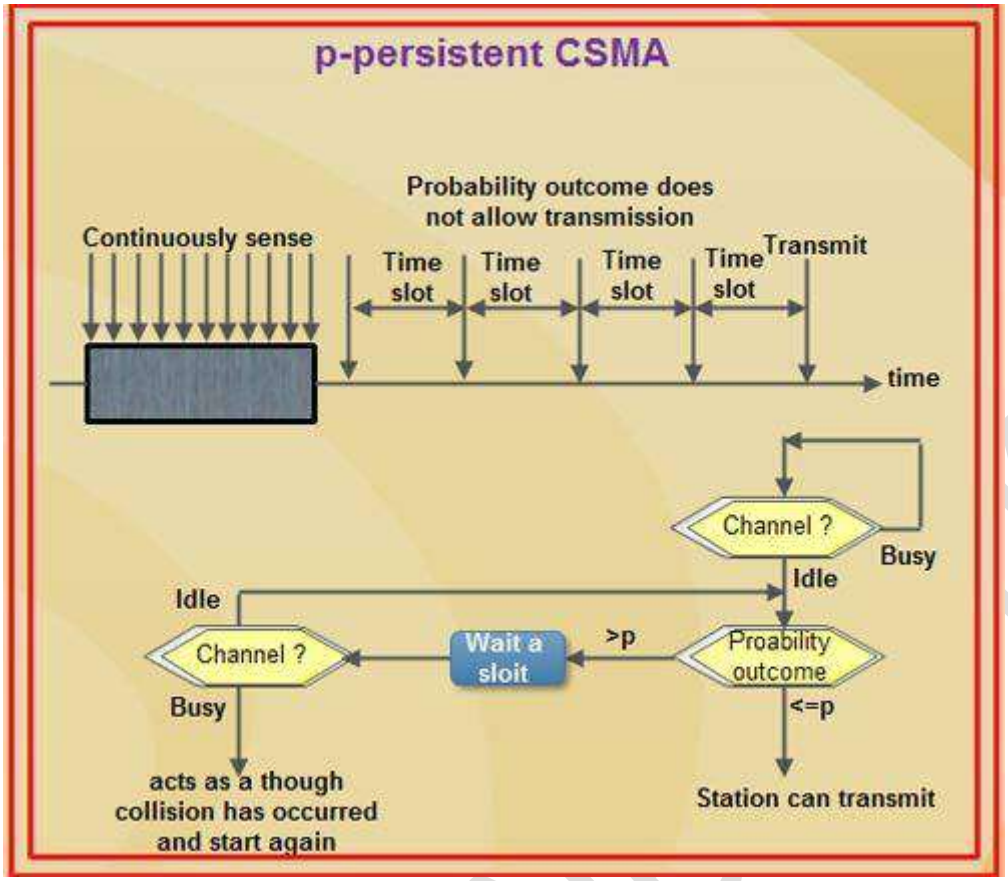


Fig 3.7 p-persistent CSMA

CSMA/CD - Carrier Sense Multiple Access / Collision Detection

To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA / CD): CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA. If the channel is busy, the station waits. it listens at the same time on communication media to ensure that there is no collision with a packet sent by another station. In a collision, the issuer immediately cancel the sending of the package. This allows to limit the duration of collisions: we do not waste time to send a packet complete if it detects a collision. After a collision, the transmitter waits again silence and again, he continued his hold for a random number; but this time the random number is nearly double the previous one: it is this called back-off (that is to say, the "decline") exponential. In fact, the window collision is simply doubled (unless it has already reached a maximum). From a packet is transmitted successfully, the window will return to its original size.

Again, this is what we do naturally in a meeting room if many people speak exactly the same time, they are realizing account immediately (as they listen at the same time they speak), and they interrupt without completing their sentence. After a while, one of them speaks again. If a new collision occurs, the two are interrupted again and tend to wait a little longer before speaking again.

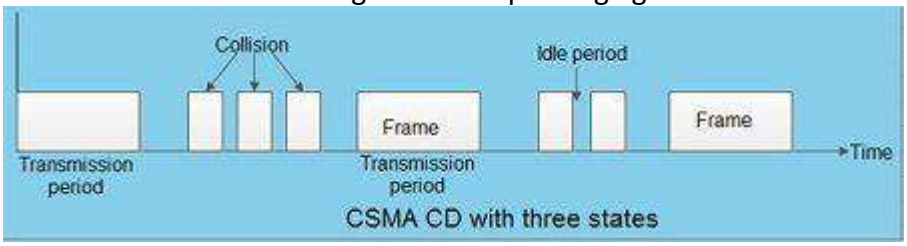


Fig 3.8 CSMA/CD

CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.

• CSMA/CA avoids the collisions using three basic techniques.

(i) Interframe space
(ii) Contention window
(iii) Acknowledgements

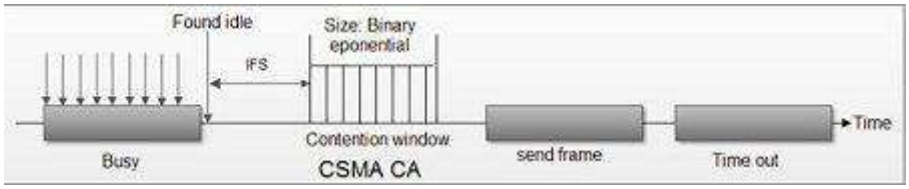


Fig 3.9 CSMA/CA

Comparision between all with an BAR Chart

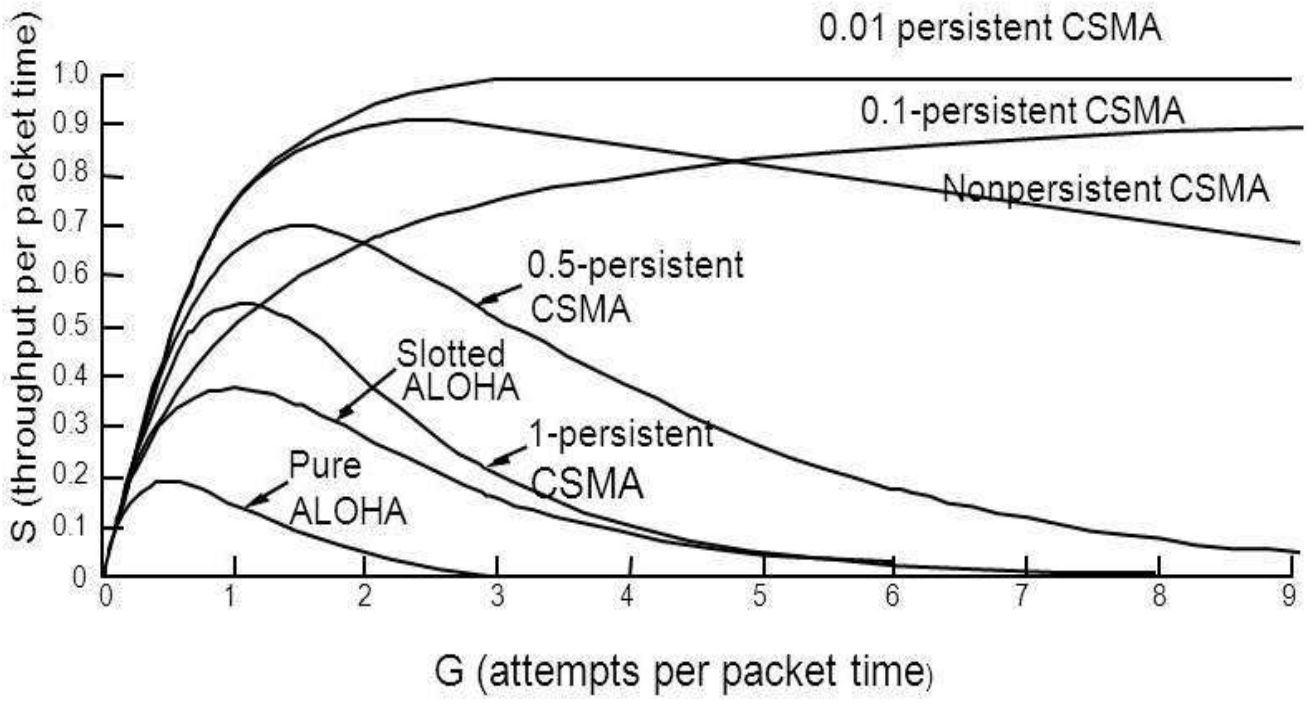


Fig 3.10 Comparision between all with an BAR Chart

1. Interframe Space (IFS)

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.

2. Contention Window

- 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.
- The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- In contention window the station needs to sense the channel after each time slot.

• If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

3. Acknowledgement

• Despite all the precautions, collisions may occur and destroy the data.

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

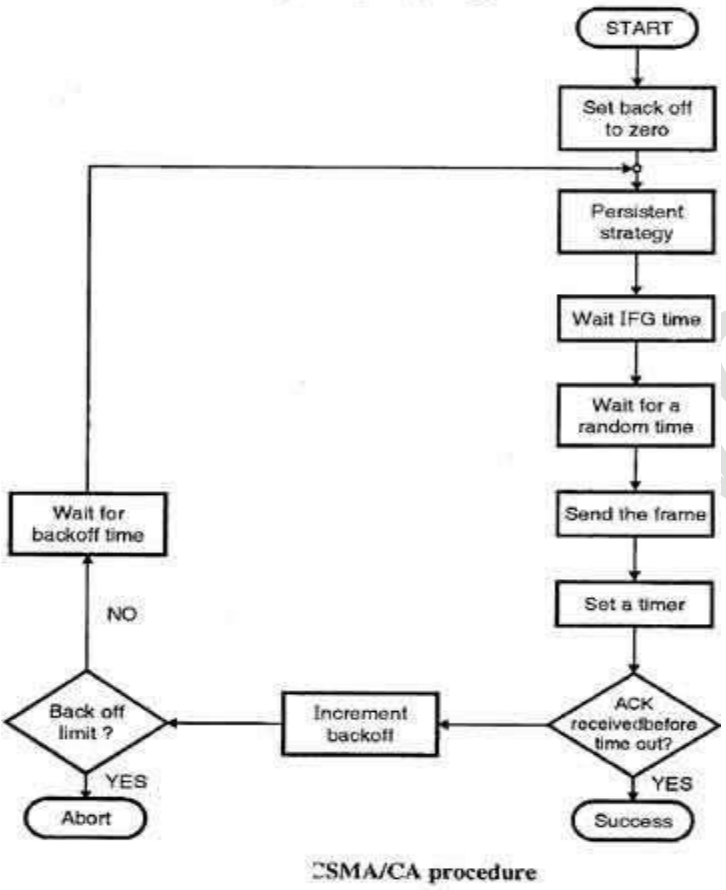


Fig 3.11 Flow Chart of CSMA/CA

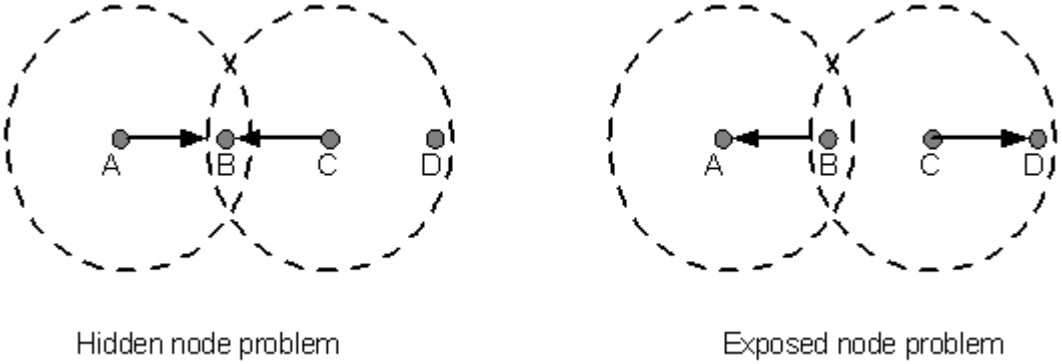
LINK: https://www.youtube.com/watch?v=74zIRH-bj2c

Hidden Node Problem

In the case of wireless network it is possible that A is sending a message to B, but C is out of its range and hence while "listening" on the network it will find the network to be free and might try to send packets to B at the same time as A. So, there will be a collision at B. The problem can be looked upon as if A and C are hidden from each other. Hence it is called the "hidden node problem".

Exposed Node Problem

If C is transmitting a message to D and B wants to transmit a message to A, B will find the network to be busy as B hears C trnasmitting. Even if B would have transmitted to A, it would not have been a problem at A or D. CSMA/CD would not allow it to transmit message to A, while the two transmissions could have gone in parallel.



Hidden node problem Exposed node problem

Fig 3.12 Hidden and Exposed Node Problem

Collision Free Protocols: Basic Bit Map, BRAP, Binary Count Down

Collision Free Protocols

A collision-free protocol for transmitting frames between stations connected over a shared transmission medium such as an IEEE 802.3 Ethernet LAN. A logical ring is formed and a token is circulated among the connected stations part of the logical ring (not all connected stations are required to be part of the logical ring). Transmitting from any one station, part of the logical ring, is permitted only while holding the token, therefore preventing collisions. A collision-free protocol, over a standard Ethernet infrastructure, becomes feasible, yet remains compatible with the standard collision protocol, thus improving performances.

Basic Bit Map

1. Assume N stations are numbered from 1 to N.
2. There is a contention period of N slots (bits).
3. Each station has one slot time during the contention period, numbered 1 to N.
4. Station J sends a 1-bit reservation during Jth slot time if it wants to transmit a frame.
5. Every station sees all the 1-bit reservation transmitted during the contention period, so each station knows which stations want to transmit.
6. After the contention period, each station that asserted its desire to transmit sends its frame in the order of station number.

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 Countdown

In this protocol, a node which wants to signal that it has a frame to send does so by writing its address into the header as a binary number. The arbitration is such that as soon as a node sees that a higher bit position that is 0 in its address has been overwritten with a 1, it gives up. The final result is the address of the node which is allowed to send. After the node has transmitted the whole process is repeated all over again. Given below is an example situation.

Nodes	Addresses
A	0010
B	0101
C	1010
D	1001

	1010

Node C having higher priority gets to transmit. The problem with this protocol is that the nodes with higher address always wins. Hence this creates a priority which is highly unfair and hence undesirable.

MLMA protocol

Multi-Level Multi-Access (MLMA): The problem with BRAP is the delay when the channel is lightly loaded. When there is no frame to be transmitted, the N-bit headers just go on and on until a station inserts a 1 into its mini slot. On average, the waiting time would be N=2. MLAM scheme 41 is nearly as efficient under high channel load, but has shorter delay under low channel load. In MLAM, a station wants to transmit a frame sends its identification in a particular format. A group of 10 bits (called decade) is used to represent a digit of the station number 48.

Limited Contention Protocols: Adaptive Tree Walk

Contention based and Contention - free has their own problems. Under conditions of light load, contention is preferable due to its low delay. As the load increases, contention becomes increasingly less attractive, because the overload associated with channel arbitration becomes greater. Just the reverse is true for contention - free protocols. At low load, they have high delay, but as the load increases, the channel efficiency improves rather than getting worse as it does for contention protocols.

Obviously, it would be better if one could combine the best properties of the contention and contention - free protocols, that is, protocol which used contention at low loads to provide low delay, but used a contention-free technique at high load to provide good channel efficiency. Such protocols do exist and are called Limited contention protocols.

It is obvious that the probability of some station acquiring the channel could only be increased by decreasing the amount of competition. The limited contention protocols do exactly that. They first divide the stations up into (not necessarily disjoint) groups. Only the members of group 0 are permitted to compete for slot 0. The competition for acquiring the slot within a group is contention based. If one of the members of that group succeeds, it acquires the channel and transmits a frame. If there is collision or no node of a particular group wants to send then the members of the next group compete for the next slot. The probability of a particular node is set to a particular value (optimum).

Adaptive Tree Walk Protocol

Initially all the nodes are allowed to try to acquire the channel. If it is able to acquire the channel, it sends its frame. If there is collision then the nodes are divided into two equal groups and only one of these groups compete for slot 1. If one of its member acquires the channel then the next slot is reserved for the other group. On the other hand, if there is a collision then that group is again subdivided and the same process is followed. This can be better understood if the nodes are thought of as being organised in a binary tree.

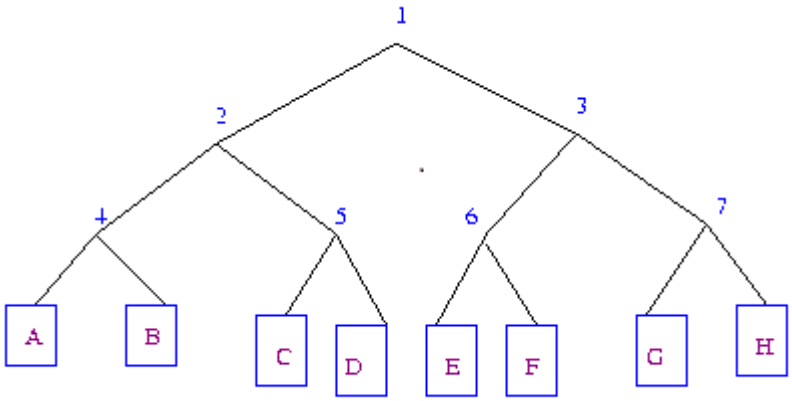


Fig 3.13 Adaptive Tree Walk

Many improvements could be made to the algorithm. For example, consider the case of nodes G and H being the only ones wanting to transmit. At slot 1 a collision will be detected and so 2 will be tried and it will be found to be idle. Hence it is pointless to probe 3 and one should directly go to 6,7.

URN Protocol

In computing, a uniform resource name (URN) is the historical name for a uniform resource identifier (URI) that uses the scheme. A URI is a string of characters used to identify a name of a web resource. Such identification enables interaction with representations of the web resource over a network, typically the World Wide Web, using specific protocols.

URNs were intended to serve as persistent, location-independent identifiers, allowing the simple mapping of namespaces into a single URN namespace. The existence of such a URI does not imply availability of the identified resource, but such URIs are required to remain globally unique and persistent, even when the resource ceases to exist or becomes unavailable.

(Uniform Resource Name) A name that identifies a resource on the Internet. Unlike URLs, which use network addresses (domain, directory path, file name), URNs use regular words that are protocol and location independent. Providing a higher level of abstraction, URNs are persistent (never change) and require a resolution service similar to the DNS system in order to convert names into real addresses. For the most part, URNs have evolved into XRI identifiers (see XDI). See URI and URL.

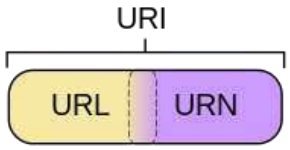


Fig 3.14 URN Protocol

High Speed LAN: Fast Ethernet, Gigabit Ethernet

Name	IEEE Standards	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Key Differences between Fast Ethernet and Gigabit Ethernet

- Gigabit Ethernet is more advanced technology than Fast Ethernet having speed of 1000 Mbit/s, 10 times more than speed of Fast Ethernet, which is 100 Mbit/s.
- Due to more bit transfer speed and higher bandwidth, Gigabit Ethernet results in better performance than Fast Ethernet.
- Gigabit Ethernet is more expensive than Fast Ethernet. Upgrading of Fast Ethernet from Standard Ethernet is easy and cost effective while upgrading of Gigabit Ethernet from Fast Ethernet is complex and expensive.
- Configuration problems in Gigabit Ethernet are more complex than Fast Ethernet. Devices used in Gigabit Ethernet must have same configuration to function fully. While in Fast Ethernet, connected devices configure automatically with the system.
- Every network can support 100 Mbit/s but cannot support 1000 Mbit/s. So, specific network is required that can support the Gigabit Ethernet.
- Maximum length of 10 km network can be achieved in Fast Ethernet, if 100BASE-LX10 version is being used. While 70 km network length can be achieved in Gigabit Ethernet, if Single Mode Fiber (1,310 nm wavelength) is being used as a medium.

- Faster Ethernet runs on both optical fiber cable and unshielded twisted pair cable. Gigabit Ethernet runs on either 1000BASE-T twisted pair cable, 1000BASE-X optical fiber or 1000BASE-CX shielded balanced copper cable.
- Fast Ethernet is economical but provides the slow transfer speed as compared to the Gigabit Ethernet that provides the faster transfer rate but is very expensive. The ports of Gigabit Ethernet cost four times the price per port of Fast Ethernet.
- IEEE Standard for Gigabit Ethernet is IEEE 802.3-2008 and the IEEE Standards for Fast Ethernet are 802.3u-1995, 802.3u-1995 and 802.3u-1995.
- Upgrade from simple Ethernet to Fast Ethernet is relatively simple and economical as compared to the upgrade from Fast Ethernet to Gigabit Ethernet.
- Gigabit Ethernet requires specifically designed network devices that can support the standard 1000Mbps data rate. Fast Ethernet requires no specific network devices.
- Manual configuration is the must-have element in the setup of Gigabit Ethernet where most of the devices required prior configuration in order to be compatible with Gigabit Ethernet. While in Fast Ethernet there is no scene of configuration as connected devices automatically configured according to the requirement of Fast Ethernet.
- If you need the more bandwidth then Gigabit Ethernet will provide you the more bandwidth at the best possible frequency as compared to the Fast Ethernet.

FDDI

The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper. It should be noted that relatively recently, a related copper specification, called Copper Distributed Data Interface (CDDI), has emerged to provide 100-Mbps service over copper. CDDI is the implementation of FDDI protocols over twisted-pair copper wire. This article focuses mainly on FDDI specifications and operations, but it also provides a high-level overview of CDDI.

FDDI uses dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. As will be discussed in detail later in this article, the primary purpose of the dual rings is to provide superior reliability and robustness.

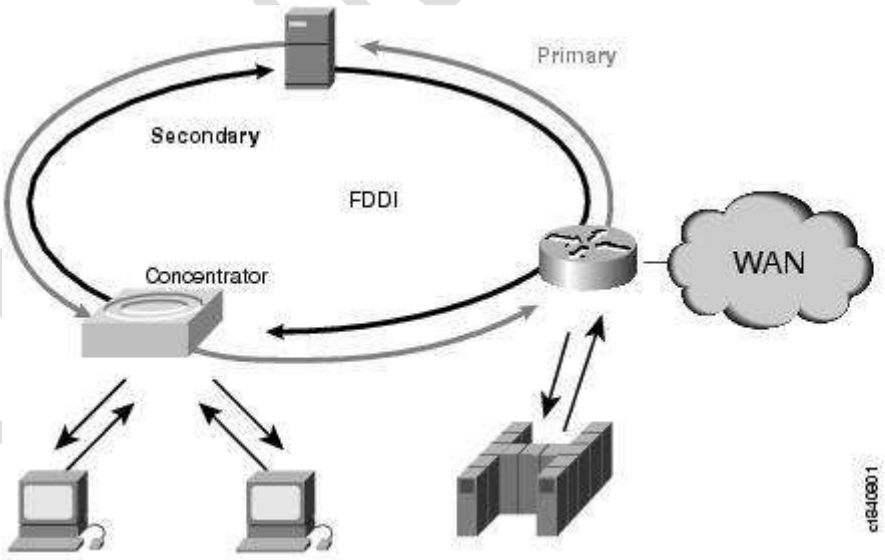


Fig 3.14 FDDI

FDDI Transmission Media

FDDI uses optical fiber as the primary transmission medium, but it also can run over copper cabling. As mentioned earlier, FDDI over copper is referred to as Copper-Distributed Data Interface (CDDI). Optical

fiber has several advantages over copper media. In particular, security, reliability, and performance all are enhanced with optical fiber media because fiber does not emit electrical signals. A physical medium that does emit electrical signals (copper) can be tapped and therefore would permit unauthorized access to the data that is transiting the medium. In addition, fiber is immune to electrical interference from radio frequency interference (RFI) and electromagnetic interference (EMI). Fiber historically has supported much higher bandwidth (throughput potential) than copper, although recent technological advances have made copper capable of transmitting at 100 Mbps. Finally, FDDI allows 2 km between stations using multimode fiber, and even longer distances using a single mode.

FDDI defines two types of optical fiber: single-mode and multimode. A mode is a ray of light that enters the fiber at a particular angle. Multimode fiber uses LED as the light-generating device, while single-mode fiber generally uses lasers.

Multimode fiber allows multiple modes of light to propagate through the fiber. Because these modes of light enter the fiber at different angles, they will arrive at the end of the fiber at different times. This characteristic is known as modal dispersion. Modal dispersion limits the bandwidth and distances that can be accomplished using multimode fibers. For this reason, multimode fiber is generally used for connectivity within a building or a relatively geographically contained environment.

Single-mode fiber allows only one mode of light to propagate through the fiber. Because only a single mode of light is used, modal dispersion is not present with single-mode fiber. Therefore, single-mode fiber is capable of delivering considerably higher performance connectivity over much larger distances, which is why it generally is used for connectivity between buildings and within environments that are more geographically dispersed.

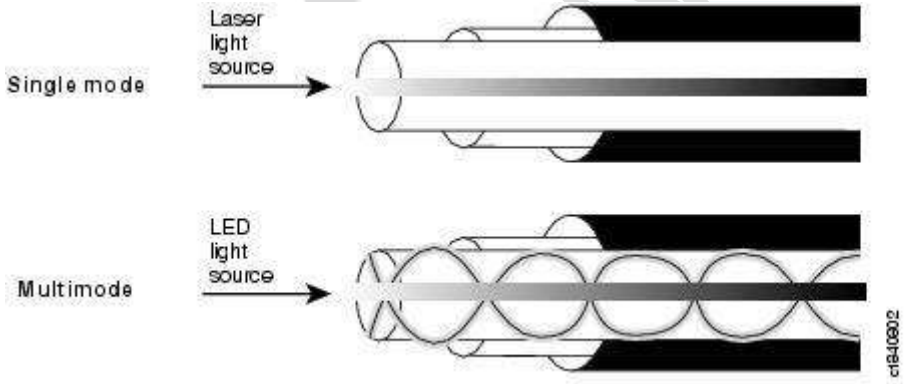


Fig 3.14 FDDI transmission medium

Performance Measuring Metrics

- **Latency:** It can take a long time for a packet to be delivered across intervening networks. In reliable protocols where a receiver acknowledges delivery of each chunk of data, it is possible to measure this as round-trip time.
- **Packet loss:** In some cases, intermediate devices in a network will lose packets. This may be due to errors, to overloading of the intermediate network, or to intentional discarding of traffic in order to enforce a particular service level.
- **Retransmission**: When packets are lost in a reliable network, they are retransmitted. This incurs two delays: First, the delay from re-sending the data; and second, the delay resulting from waiting until the data is received in the correct order before forwarding it up the protocol stack.
- **Throughput:** The amount of traffic a network can carry is measured as throughput, usually in terms such as kilobits per second. Throughput is analogous to the number of lanes on a highway, whereas latency is analogous to its speed limit.

IEEE Standards 802 series & their variant

802.2 Logical Link Control

The technical definition for 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers)."

802.2 "specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).

Basically, think of the 802.2 as the "translator" for the Data Link Layer. 802.2 is concerned with managing traffic over the physical network. It is responsible for flow and error control. The Data Link Layer wants to send some data over the network, 802.2 Logical Link Control helps make this possible. It also helps by identifying the line protocol, like NetBIOS, or Netware.

The LLC acts like a software bus allowing multiple higher layer protocols to access one or more lower layer networks. For example, if you have a server with multiple network interface cards, the LLC will forward packers from those upper layer protocols to the appropriate network interface. This allows the upper layer protocols to not need specific knowledge of the lower layer networks in use.

802.3 Ethernet

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.

Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.

The most common topology for Ethernet is the star topology.

802.5 Token Ring

Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.

The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fibber.

Token ring can be run over a star topology as well as the ring topology.

There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber.

Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

802.11 Wireless Network Standards

802.11 is the collection of standards setup for wireless networking. You are probably familiar with the three popular standards: 802.11a, 802.11b, 802.11g and latest one is 802.11n. Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.

802.11a was one of the first wireless standards. 802.11a operates in the 5Ghz radio band and can achieve a maximum of 54Mbps. Wasn't as popular as the 802.11b standard due to higher prices and lower range.

802.11b operates in the 2.4Ghz band and supports up to 11 Mbps. Range of up to several hundred feet in theory. The first real consumer option for wireless and very popular.

802.11g is a standard in the 2.4Ghz band operating at 54Mbps. Since it operates in the same band as 802.11b, 802.11g is compatible with 802.11b equipment. 802.11a is not directly compatible with 802.11b or 802.11g since it operates in a different band.

Wireless LANs primarily use CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance. It has a "listen before talk" method of minimizing collisions on the wireless network. This results in less need for retransmitting data.

Wireless standards operate within a wireless topology.

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