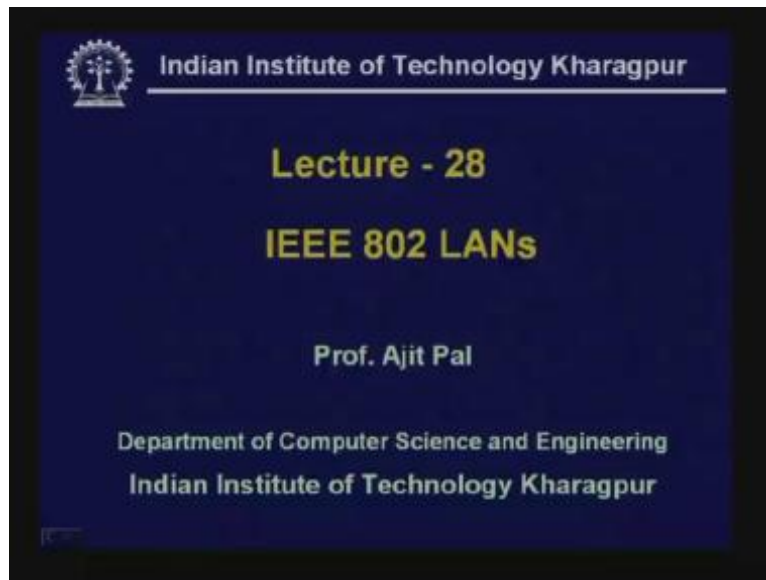


**Data Communication**  
**Prof. A. Pal**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture # 28**  
**IEEE 802 LANs**

Hello and welcome to today's lecture on IEEE 802 LANs.

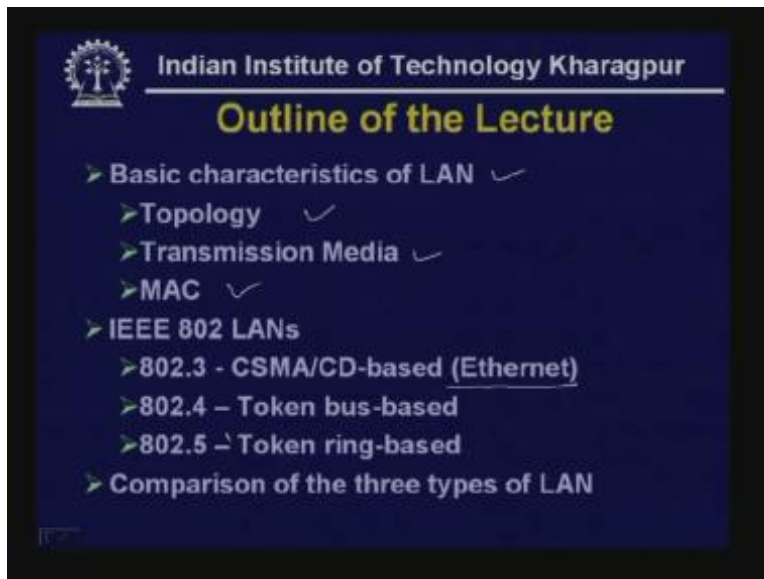
(Refer Slide Time: 01:00)



In the last lecture we have discussed about the various applications of medium access control techniques. One of the important applications of medium access control techniques is in local area networks. In this lecture I shall introduce to you the first set of standards which were developed by the IEEE 802. Here is the outline of today's lecture.

First I shall consider the basic characteristics of LAN particularly the topology, transmission media and medium access control. These are the three parameters which characterizes a local area network. Then I shall discuss about the three standards which were developed by IEEE 802 (( )) which are known as IEEE 802.3 that is based on CSMA/CD and the most popular version of it is known as Ethernet. Another is based on token bus known as IEEE 802.4 and the third one which we shall discuss today is IEEE 802.5 which is token ring based.

(Refer Slide Time: 02:10)



So we shall discuss about these three different types of local area networks and compare the performance of these three types of LANs at the end.

On completion, the students will be able to explain, the basic characteristics of local area networks, they will be able to explain the operation of IEEE 802 local area networks, first one is IEEE 802.3 based on CSMA/CD, the second one is IEEE 802.4 based on token bus, the third one is IEEE 802.5 based on token ring and they will be able to compare the performance of these three LANs.

(Refer Slide Time: 03:10)



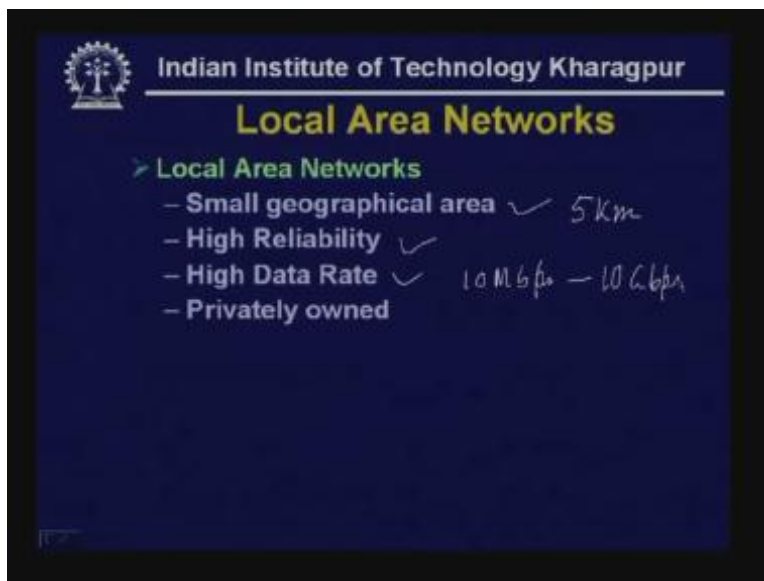
First of all let us define what we mean by local area networks.

Earlier we have discussed about the packet switched networks where the network can span over a very large geographical area known as wide area networks. On the contrary local area networks cover a very small geographical area, it can be a room, a campus, a building so it does not cover a very large area may be 5 km wide on both directions of three kilometer wide on both directions so small geographic area is one of the key features of local area networks.

Second important feature is high reliability. In wide area network in packet switched networks we have seen that because the medium used is not very reliable the standard telephone network using twisted-pair the reliability is very poor. On the other hand in local area network we shall see it uses very reliable media like optical fiber, coaxial cable and of course it uses twisted-pair but of a very small segment length so as a result it is very reliable. So the need for error detection and correction is minimal here particularly error correction is not used however error detection is provided as part of this scheme as we shall see.

Then it allows high data rate. we have seen that the packet switched networks the wide area networks do not have very high speed although over the years this speed has increased but as we shall see the local area network will have very high speed starting with may be 10 Mbps to nowadays 10 Gbps. So you see the local area networks offer very high speed.

(Refer Slide Time: 05:25)



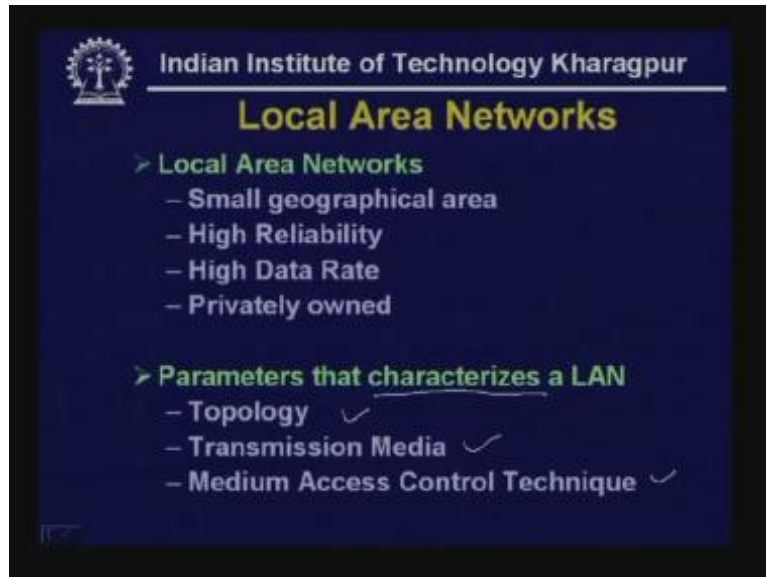
Another important characteristic is that local area networks are privately owned, wide area networks are usually owned by state that is the government. Of course nowadays many private companies are also owner of wide area networks but that is the normal situation. On the contrary local area networks are privately owned that means it can be owned by a single person or an organization or academic or government industry

whatever it is. So these are the typical characteristics of local area networks or typical features of local area networks.

Question arises how do you characterize a LAN?

There are three important parameters. The topology, transmission media and medium access control techniques. These three parameters characterize a LAN.


(Refer Slide Time: 06:25)



We shall see what are the various alternatives available so far as topology is concerned, transmission media is concerned and medium access control technique is concerned. First let us start with the topology.

The topology of a network defines how nodes and stations are connected. That means as you know in a local area network you have to connect a number of computers or stations. It need not be computers, it can be peripherals and other communication equipments like (( )) cell phones and so on. Hence, there are three important topologies which are shown here.

(Refer Slide Time: 09:00)

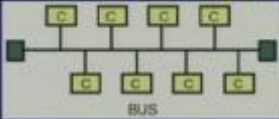
 Indian Institute of Technology Kharagpur

## Topology


> Topology defines how nodes/stations are connected

> Typical LAN topologies:

- > **Bus/ Tree**
  - All nodes are connected to a common medium
- > **Star**
  - All nodes are connected to a central node
- > **Ring**
  - Nodes form a ring by point-to-point links to adjacent neighbours.

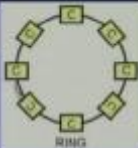


BUS



STAR

*Hub/ Switch*



RING

*Shared Media*

First one is bus in which there is a shared media and that shared media is shared by all the nodes. That means all the computers or stations are directly connected to the bus. It is similar to that electrical line distribution. All the electrical equipment are connected to the electrical bus so it is somewhat like that. We shall see how different computers can be connected to a common bus, so here all nodes are connected to a common media. So we can say you require a single segment of the medium in this particular case.

Another alternative is star which is also commonly used. Here all nodes are connected to a central node. As you can see here you have got a central node through which all the computers are connected, that central node can be a hub or it can be a switch through which different computers or other equipments can be connected. **Later on we shall discuss about it in more detail.** So you have got a central node through which all the communication take place and as you can see it appears like a star and that's why it is called star topology.

The third alternative is in the form of a ring where nodes form a ring by **point to** point links to the adjacent neighbors. Here as you can see each computer or station is connected to its neighbor with the help of point to point links and point to point links ultimately forms a ring so all the computers are connected in the form of a ring. Later on we shall see how they communicate with each other.

Now as we shall see there are varieties of transmission media that can be used, the most popular is the twisted-pair although it has got the minimum bandwidth but it serves the purpose in many situations. The second alternative is coaxial cable which is widely used then the third option is optical fiber. The optical fiber is gradually becoming more and more popular because of its very high bandwidth as you know, optical fiber is widely used nowadays in local area networks and the last alternative is the wireless communication. We shall see how different alternatives are possible for wireless transmission.

There is a close relationship between the topology and transmission media. The transmission media that we choose sometimes dictates what kind of topology that can be used. Or you can say the other way, for a particular topology some special types of transmission media is suitable. For example, for BUS, coaxial cable is the media which is the most suitable and coaxial cable is used whenever BUS topology is used.

(Refer Slide Time: 10:35)

Indian Institute of Technology Kharagpur

### Transmission Media

Transmission medium

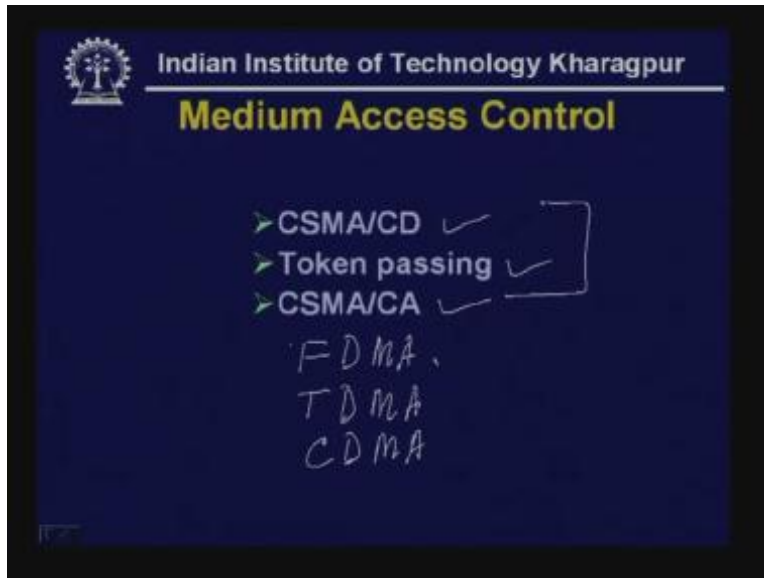
- Twisted-pair, coaxial cable, optical fiber, wireless

Topology	Transmission media
BUS	Coaxial
Ring	Twisted-pair, Optical Fiber,
Star	Twisted pair, Optical fiber

On the other hand, for ring it is possible to use twisted-pair, optical fiber but also it is possible to use coaxial cable if coaxial cable is necessary. On the other hand, for star topology it is possible to use twisted-pair and optical fiber; these are the most commonly used medium. So we find that there is some relationship between the topology and transmission medium and for different LANs these combinations are used.

Finally we come to the third important parameter that is the medium access control technique that is being used. We have already discussed different types of medium access control techniques. The most popular medium access control that is being used in CSMA/CD, token passing, CSMA/CA and of course there are other medium access control techniques like FDMA, TDMA, CDMA which are also used but for the three different types of LAN that we shall discuss today we shall find that these are the two techniques we shall use.

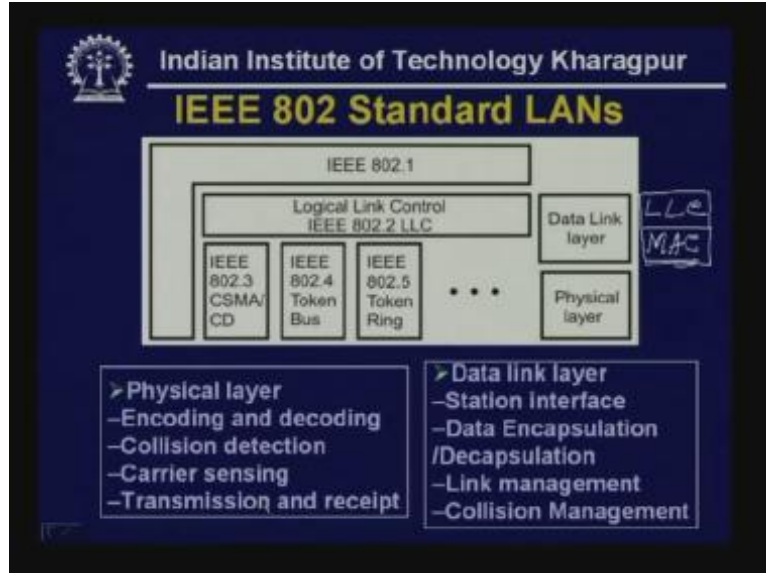
(Refer Slide Time: 11:56)



Hence, these are the various alternatives of medium access control techniques which are used in different types of local area networks. Now let us focus on the IEEE 802 standard LANs. Now IEEE 802 committee has developed three different standards namely IEEE 802.3, IEEE 802.4, IEEE 802.5. Now all these three standards share two common sublayers. First one is IEEE 802.1. This IEEE 802.1 essentially introduces different types of LANs and also it serves some kind of internetworking purpose. So it is essentially used for internetworking and also as an interface to the upper layers. Then you have got logical link control which is essentially part of the data link layer of the OSI model. Similarly, the data link layer has been divided into two sub layers in IEEE 802; one is your logical link control LLC and another is Medium Access Control MAC.

Then the lower part is the physical layer and here are the different functions performed by the two different layers, the data link layer and the physical layer. The physical layer performs the encoding and decoding. As you know, whenever you send digital signal you have to perform some kind of encoding, Manchester encoding and different types of encodings are used, so that encoding and decoding is done, then you have to perform collision detection, carrier sensing if you use CSMA/CD or CSMA/CA.

(Refer Slide Time: 14:05)



Then of course you have to do transmission and receipt of packets since these are the functions of physical layer which directly interfaces with the medium. Then the data link layer which is above the physical layer performs station interface, it performs the data encapsulation and decapsulation. As we shall see it will form some kind of frame so that it is possible to perform synchronization and other functions, then it does link management and collision management.

So, whenever collision takes place it does the management so that it comes out of the collision and also it performs link management. These are the three different types of standards.

First we shall focus on the IEEE 802.3 specification which is based on CSMA/CD. Let us first focus on the physical layer. So, in the physical layer it supports different types of transmission media. The types of transmission media that it supports varies from twisted-pair to optical fiber. It is concisely represented in the form of 10Base5 or 10Base2 or 10Base3 or 10BaseF.



(Refer Slide Time: 15:37)

The slide is titled "IEEE 802.3 Specifications" and is from the Indian Institute of Technology Kharagpur. It is divided into three main sections:

- Physical layer:**
  - 10Base5 → thickwire coaxial
  - 10Base2 → thinwire coaxial (cheapernet)
  - 10BaseT → twisted pair
  - 10BaseF → fiber optic
  - 10Broad36 - coaxial
- Table:**

10 Base	Max segment length	Nodes per segment
5	500m	100
2	185m	30
T	100m	1024
F	2000m	1024
- Signaling:**
  - Manchester in baseband
  - Differential PSK in broadband

This 10 specifies the data rate that means data rate is 10 Mbps so this ten signifies the data rate and this base specifies whether it is base band or broad band. So in this particular case 10Base means baseband, however, there is a possibility of using broadband in such a case it will be ten broad thirty six coaxial so in this case it is a broad band communication.

On the other hand for all these options which are shown here it is 10Base5. What is a significance of this number five? Here five signifies that each segment of the cable can be 500 meters in length so it signifies the maximum segment length. For example, for the first option it is 10Base5 which is a thick wire coaxial cable, then 10Base2 which uses thick wire coaxial cable, then 10Base2 which uses thin wire coaxial cable is also known as cheapernet that can use a maximum segment length of 185 m which is rounded up to 2.

Then the third medium used is twisted-pair and the maximum segment length is hundred meter. And the fourth one is optical fiber that is your multimode fiber is being used here, and the maximum length is 2000 m or 2 km and on each segment you can have different number of nodes or computers you can say. For example, in 10Base5 you can have hundred computers, in 10Base2 you can have thirty computers on a single segment and on 10BaseT you can have 1024 computers and on 10BaseF you can have 10024 computers. And whenever you are using broadband of course the number is 1024 and the length is 36 m.

The signaling used in different situations are here. For baseband the signaling that is used is Manchester. We know that Manchester encoding helps you to synchronize the clock at the receiving end that's why Manchester encoding is used in IEEE 802 or Ethernet which is similar to IEEE 802.3. On the other hand, whenever broad band signal is used, differential phase shift keying is used and of course the use of this is not very popular.

The baseband signal is most popular that's why we shall mainly focus on the baseband signaling and networks based on baseband signal.

Let us consider the four cases that is used in IEEE 802.3. First one is 10Base5, 10 stands for 10 Mbps baseband transmission, the standard specifies 0.5 inch coaxial cable known as yellow cable or thick Ethernet like the cable used as hose pipe or something that is used for gardening. Each cable segment can be a maximum of 500 m long and this 5 (Refer Slide Time: 19:22) signifies that and up to maximum of five cable segments can be connected using repeaters with maximum length of 2500 m.

That means you can have a number of segments connected with the help of repeaters. So you can put a repeater and then connect to such segments. In this way you can have four such repeaters in between and connect five such segments in cascade to have a maximum length of 2500 m. And as I mentioned at most 1024 stations per Ethernet network is allowed however on each segment the number is only hundred. So on each segment you can have hundred nodes or (( ))

(Refer Slide Time: 20:09)

**Indian Institute of Technology Kharagpur**

## 10Base5

- Supports 10 Mbps baseband transmission.
- The standard specifies 0.5 inch coaxial cable, known as **yellow cable or thick Ethernet**.
- Each cable segment can be maximum 500 meters long.
- Up to a maximum of 5 cable segments can be connected using repeaters, with maximum length 2500 meters.
- At most 1024 stations per Ethernet network is allowed.

Some characteristics:

- Used for backbone networks
- Tap: cable need not be cut
- Transceiver: send/receive, collision detection, electronic isolation
- AUI: Attachment Unit Interface

Now let us see how exactly this 10Base5 works, and how the cabling is done. This is that coaxial cable that yellow coaxial cable of 0.5 inch diameter which is running and to connect one computer a transceiver is firmly attached to the cable and a vampire hole is made called tap, the vampire tap is made which goes to almost half the coaxial cable. That means it touches the inner portion of the core conductor so now the core conductor is connected and the upper conductor is in the form of **gradedness**. So these two are connected to a transceiver which is directly connected from the attached cable and from that transceiver one cable Attachment Unit Interface AUI cable is connected comes to the computer and in the computer you have got a Network Interface Card or NIC to which the computer is either built in as part of the mother board or there is a separate card.

The AUI cable can be 50 m in length. This is how a computer can be connected in the case of a 10Base5 standard. This is the 500 m segment (Refer Slide Time: 21:58) and at both ends we have got a terminator, this terminator is very important as it prevents signal reflection at the other end. This is one segment and whenever a computer is to be connected a vampire type is made and a transceiver is attached and from that transceiver AUI cable goes to the computer. This is how through this coaxial cable different computers can be connected. In this diagram two computers connected with the help of two transceivers.

(Refer Slide Time: 22:25)

**Indian Institute of Technology Kharagpur**

### 10Base5

- Supports 10 Mbps baseband transmission.
- The standard specifies 0.5 inch coaxial cable, known as **yellow cable or thick Ethernet**.
- Each cable segment can be maximum 500 meters long.
- Up to a maximum of 5 cable segments can be connected using repeaters, with maximum length 2500 meters.
- At most 1024 stations per Ethernet network is allowed.

**Some characteristics:**

- Used for backbone networks
- Tap: cable need not be cut
- Transceiver: send/receive, collision detection, electronic isolation
- AUI: Attachment Unit Interface

*Vampire tap*

*NIC 50m*

So the transceiver does send and receive collision detection, electronic isolation and the other function is done by the network interface card which is connected to the motherboard of the computer. This is how the 10Base5 works.

On the other hand, the 10Base2 also supports 10 Mbps baseband transmission, the standard specifies zero point two five inch coaxial cable known as cheapernet or thin Ethernet. So here the coaxial cable is of cheaper variety which is used in cable TV which is 0.25 inches in diameter and that's why it is also called chapernet because of its lower cost and also it is called thin Ethernet because this diameter is thinner than the standard 10Base5.

So here **as I have mentioned** actually 185 m is the maximum segment length and up to five cable segments can be connected using repeaters with maximum length of 925 m. So in this way with five repeaters you can have 925 m and total number of computers is the same which is 1024.

This is connected in this manner (Refer Slide Time: 24:05). Whenever a computer has to be connected the coaxial cable is cut and a BNC T type connector is attached at both ends of the cut cable and that can be connected to the Network Interface Card which is

available in the form of T. So this T connector is essentially connected to the network interface card and then these two which are connected to ends of the cable can be connected to the network interface card.

(Refer Slide Time: 24:38)

The slide features the IIT Kharagpur logo and title. The main heading is '10Base2' with a handwritten '← 185' next to it. A list of bullet points describes the standard, including its 10 Mbps baseband transmission, 0.25 inch coaxial cable (labeled 'cheapernet or thin Ethernet' and 'Cable TV'), and segment length limits (185m per segment, 925m total with repeaters). A box lists characteristics: office LAN use, BNC connectors, and no drop cables. A diagram shows a BNC T connector connecting a central hub to a computer.

Indian Institute of Technology Kharagpur

### 10Base2 ← 185

- Also supports 10 Mbps baseband transmission.
- The standard specifies 0.25 inch coaxial cable known as **cheapernet or thin Ethernet**. *Cable TV*
- Each cable segment can be maximum 185 m long.
- Up to a maximum of 5 cable segments can be connected using repeaters, with maximum length of 925 meters. *1024*

➤ Some characteristics:

- Use for office LAN / departmental LAN
- BNC connector
- No drop cable

BNC T Connector

So in this way this thin Ethernet cable can (( )) through the entire building or entire floor and can go from one computer to another computer having a BNC T connector for each of the computer.

Then comes the 10BaseT which again supports ten mega bits baseband signaling. Here it uses twisted-pair. **As I mentioned** the twisted-pair can be used both for category 3 or category five cables and it requires a hub or the hub in the centre node. The hub is essentially multiport repeater. That means whatever signal is present here are also present in all the ports and the stations are connected with the help of a RJ-45 connector. That means the twisted-pair cable is connected with the help of a RJ-45 connector and maximum length of each of these segments can be at most 100 m as you can see.

You may be asking why we have deviated from using coaxial cable. Actually in case of 10Base5 or 10Base2 there is always a problem of loose connection, cut and other problems and for that purpose time domain reflectometry is used for detection of fault which is very time consuming. So, that problem can be avoided in case of this hub based 10BaseT Ethernet network wherein it is very easy to maintain and diagnose a fault. That's why this particular topology has become very popular.

(Refer Slide Time: 26:25)

Indian Institute of Technology Kharagpur

### 10BaseT

- Supports 10 Mbps baseband transmission.
- The standard specifies the 24AWG Unshielded Twisted Pair (UTP)
  - Both Cat-3 and Cat-5 cables may be used
- A HUB functions as a repeater
- Stations connect to the hub with RJ45 connector
- Maximum segment length is 100 meters
- Easy to maintain and diagnose

Multipoint Repeater

Now another alternative as I mentioned is 10BaseF where F stands for fiber. We can use 10Base fiber particularly when the distance longer. There are three alternatives; 10BaseFP a passive star topology is used which allows up to 1 Km length and 10BaseFL which is the most popular asynchronous point-to-point link which gives you up to 2 Km and third alternative is 10BaseFB a synchronous point-to-point link which also gives up to 2 km with 15 cascaded repeaters that can be used in this particular case.

(Refer Slide Time: 27:15)

Indian Institute of Technology Kharagpur

### 10BaseF

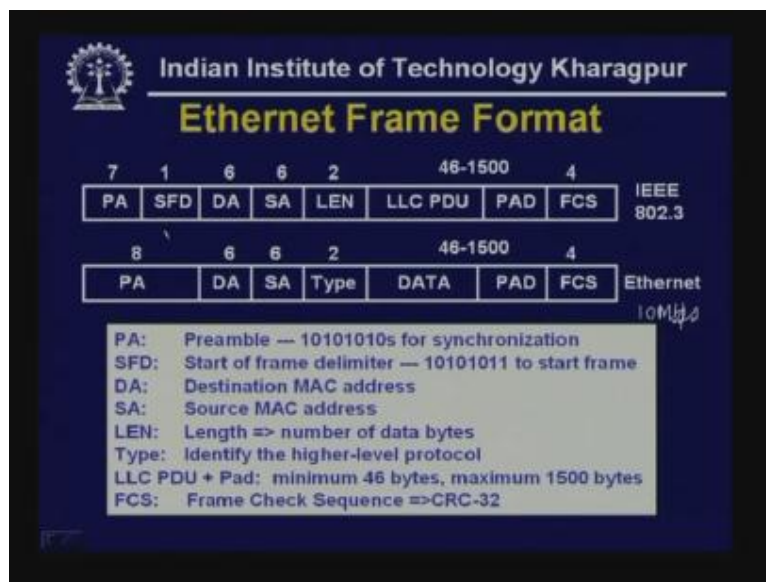
- Allows long distance connections using optical fiber
  - 10BaseFP → A passive-star topology, up to 1 Km link
  - 10BaseFL → An asynchronous point-to-point link, up to 2 Km
  - 10BaseFB → A synchronous point-to-point link, up to 2 Km with 15 cascaded repeaters

So we have seen various alternatives of the Ethernet or **IEEE 802.2**. So, as I mentioned Ethernet and IEEE 802 are not really the same. Ethernet was the standard developed by

(.....rox, (Derc... 27:34) and Intel and IEEE 802 was developed based on Ethernet. sometimes whenever IEEE 802 is mentioned we refer it to Ethernet but they are not exactly same, Ethernet was the standard developed by the three companies (.....rox, (Derc...and intel, on the other hand, IEEE 802.3 was developed by IEEE 802 committee, however, they are very similar.

As you can see there is some dissimilarity in the same format, there is a preamble, preamble is a sequence of alternative one zeroes and since it uses Manchester encoding the consecutive one zeroes appear as 10 Mbps square ...s in the receiving end and the receiver can do the synchronization.

(Refer Slide Time: 27:15)



Then in IEEE 802.3 there is a start frame delimiter which is opened by that means 10101011 which signifies the start of a frame. So synchronization is done with the help of these 7 bytes. That means 7 into 856 alternate bits like the 1010 bits. Then it uses the source address ,destination medium access control address, source media access control address and this destination address and source address are essentially 48-bit as you can see the total length is 48-bit, this is the MAC address.

The first two bits is meant for individual address, if it is 1 it is meant for group address and whenever this cell bit is 0 then it is meant for global administered address and 1 stands for local administered address.

(Refer Slide Time: 29:45)

Indian Institute of Technology Kharagpur

## Ethernet MAC Address

I/G U/L 46-bit address

← 48 bit →

I/G = 0 → individual address  
= 1 → group address  
U/L = 0 → global administered address  
= 1 → local administered address

**Unicast:** Defines a single destination  
**Broadcast:** FFFFFFFF each station on the network receive and accept frames  
**Multicast:** A group address defines multiple recipient

Therefore, with the help of these two bits it defines the nature whether it is meant for unicast, broadcast or multicast and with the help of these 46 bits it allows large number of global addresses that is  $7$  into  $10$  to the power  $13$ . So it allows you have to so many addresses to be used in case of Ethernet and this is a fixed address which is being used in this case. Of course the IEEE 802.3 standard originally allowed both  $2$  byte address and  $6$  byte address but  $6$  byte address is the most popular and LEN stands for the length of the number of data bytes. As you can see here (Refer Slide Time: 30:32) it differs from Ethernet.

(Refer Slide Time: 30:34)

Indian Institute of Technology Kharagpur

## Ethernet Frame Format

7	1	6	6	2	46-1500	4	
PA	SFD	DA	SA	LEN	LLC PDU	PAD	FCS
							IEEE 802.3

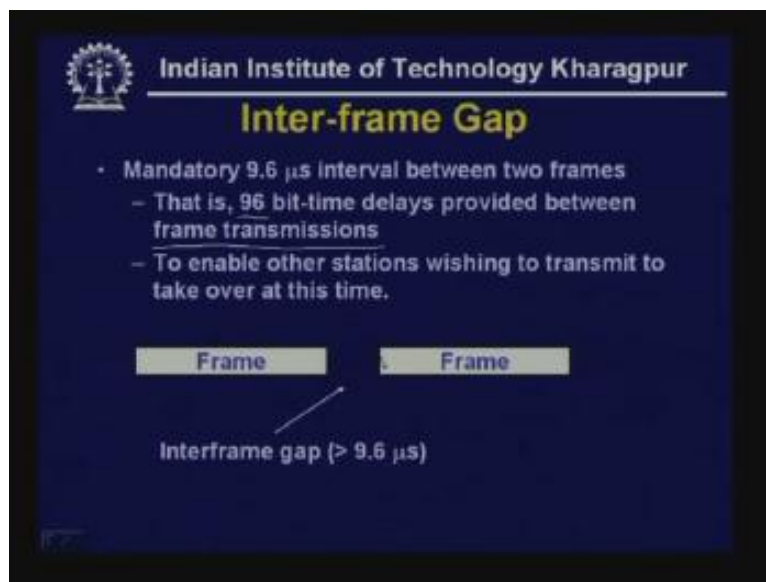
  

8	6	6	2	46-1500	4		
PA	DA	SA	Type	DATA	PAD	FCS	
							Ethernet

PA: Preamble — 10101010s for synchronization  
SFD: Start of frame delimiter — 10101011 to start frame  
DA: Destination MAC address  
SA: Source MAC address  
LEN: Length => number of data bytes  
Type: Identify the higher-level protocol  
LLC PDU + Pad: minimum 46 bytes, maximum 1500 bytes  
FCS: Frame Check Sequence => CRC-32

In case of Ethernet it defines the type of the higher level protocol. On the other hand, in IEEE 802.3 it specifies the number of data bytes. So here is a number of data bytes. The data bytes can vary from 46 to 1500. You may be asking why 46? The reason for that is, there is a restriction on minimum length of the frame and if the data byte is 0 then a 46 byte pad is introduced. That's why whenever the data byte is 0 there is a 46 byte pad. On the other hand, if the data byte itself is more than 46 byte then it can be only the data byte and no pad is necessary. And finally there is a frame check sequence which uses the CRC 4 byte that is 32 byte cyclic redundancy code for error detection. Therefore, as you can see in LAN in IEEE 802 error detection was allowed once provided. There is another important point.

(Refer Slide Time: 32:20)

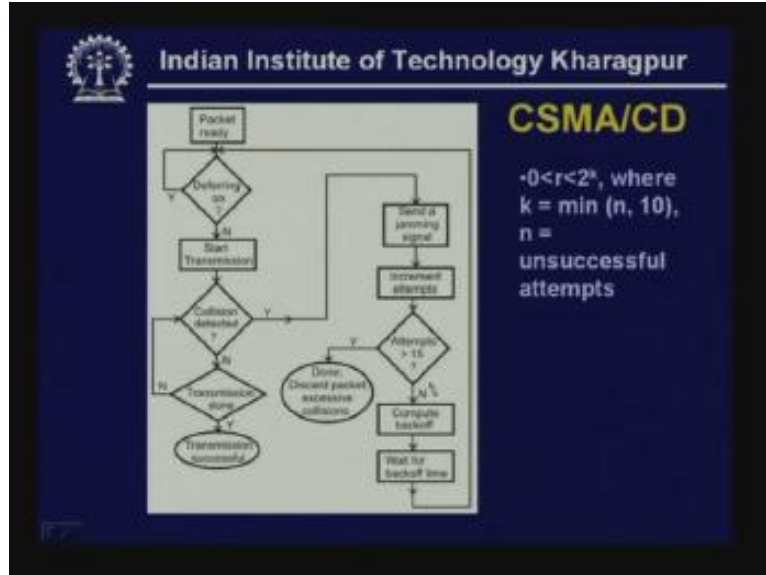


As you can see in this diagram, between two frames there is a mandatory gap of 9.6 micro seconds. This gap is allowed which is essentially 96-bit time delays provided between frame transmissions. This is provided to enable other stations wishing to transmit to take over at this time. For example, one frame transmission is over and before another frame can be transmitted this gap is allowed so that other stations can send their frame.

Of course there is a possibility of collision. We have already discussed about how this binary exponential backoff algorithm is used whenever there is collision or multiple collisions and we now discuss it here at this point. Hence, using this binary exponential backoff algorithm it comes out of the collision if possible, otherwise after sixteen attempts that is 1 plus 15 collision attempts it comes out and the packet is discarded.



(Refer Slide Time: 32:54)



Now there are some important points to be discussed about the collision detection. As you know a station sends a frame and while sending it senses the media and collision is detected each station senses exceeded the signal strength. That means essentially it is done by some kind of analog signaling by analog circuit. If the signal level is higher then it detects a collision particularly in coaxial cable. On the other hand, whenever the twisted-pair is used then of course you are using some kind of a hub, so, if there is signal on more than one port that means there is collision. This is how collision is detected.

Whenever a collision occurs what the station does? The transmitting station sends a jamming signal after collision is detected which can be either 32-bit jamming signal of alternative ones and zeroes or 48-bit jamming signal.

(Refer Slide Time: 34:05)

**Indian Institute of Technology Kharagpur**

## Collision Detection

- How are collisions detected?
  - A station sends frame and senses the medium
  - Collision is detected if station senses exceeded signal strength (coaxial cable)
  - There is signal on more than one port (UTP)
- What the station does?
  - Transmitting stations send a jamming signal after collision is detected.
  - 32-bit jam signal → 10101010 --- 10101010
  - 48-bit jam signal → 10101010 --- 10101010
- The jam signal serves as a mechanism to cause non-transmitting stations to wait until the jam signal ends.

So this jamming signal serves as a mechanism to cause non transmitting stations to wait until the jam signal ends. That means the transmitting stations that have suffered collision will send the jamming signal so that jamming signal will alert the other stations so that they will wait until the jamming signal is over before starting transmission.

Now as I mentioned there is a concept of minimum frame size. How it occurs? The reason for that comes from this particular situation as you can see. A starts transmission at time  $t$  is equal to 0 and before it reaches the other end the B starts transmission and of course when this end reaches there is a collision here and that collision is detected by B and when this also reaches A there is a collision. So depending on the propagation time, if  $\tau$  is the propagation time a frame must take more than  $2\tau$  that is two times the propagation time for detection of collision.

Now, in terms of slot time, this corresponds to 51.2 micro second, this is corresponding to 512 bytes that means it assumes that it is whenever you have got a maximum number of segments connected by repeaters, so this is a repeater here in other segment (Refer Slide time: 35:47) in this way you can have a number of segments cascaded and then the end to end delay is two times the end of delays so 51.2 micro seconds is assumed. So this corresponds to 512 byte.

(Refer Slide Time: 35:55)

Indian Institute of Technology Kharagpur

### Minimum Frame Size

- A frame must take more than  $2\tau$  time to send
  - For preventing the situation that the sender incorrectly concludes that the frame was successfully sent.
- This slot time is  $51.2\mu\text{sec}$  corresponding to  $512$  bit = 64 bytes
  - Minimum frame length is 64 bytes Data field must have 46 bytes minimum

1. 6 μsec transmission at 10 Mb/s  
2. 6 μsec transmission at 10 Mb/s  
3. 6 μsec collision at 10 Mb/s  
4. 6 μsec collision at 10 Mb/s

You require the frame size a minimum of sixty two bytes. Of course the other parts are there. For example, you have got the other parts so 6 plus 6 plus 2 plus 4 so if you add these two 12, 14 then 20 and if you subtract 18 that is 6 plus 6 is equal to 12, 14, 18 from 64 you will get 46, that's how the 46 comes.

So we have seen the need for the minimum frame size of 64 bytes. However, if there is a collision there is a possibility of late collisions that take place after 64 bytes so that can happen because of excessive cable length or too many repeaters or faulty connector of defective network interface card.

(Refer Slide Time: 37:00)

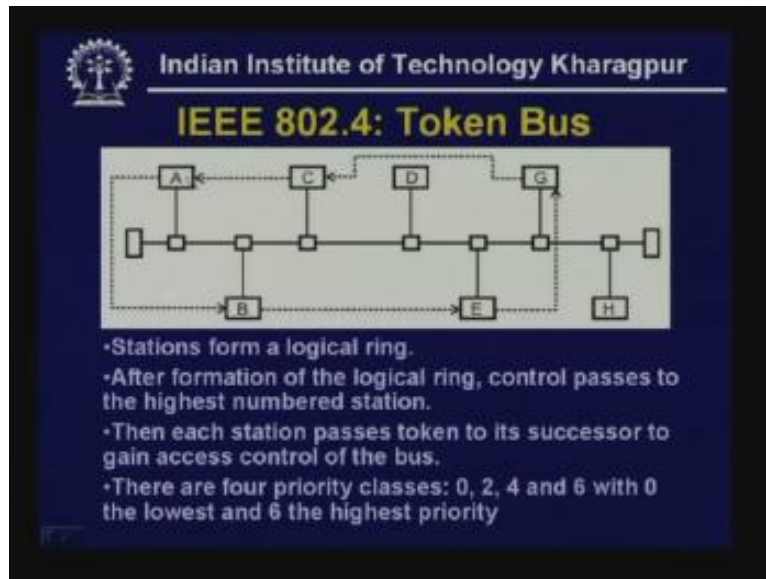
Indian Institute of Technology Kharagpur

### Late Collision

- Late collisions are collisions that take place after the first 64 bytes of a frame have been transmitted.
  - Sender will incorrectly conclude that the frame was successfully sent.
- Primary causes:
  - Excessive cable lengths ✓
  - Too many repeaters ✓
  - Faulty connector or defective NIC ✓

This can happen in abnormal situations otherwise all the collision will occur within the transmission time of 64 bytes, that's why the minimum length of the packet is provided and during the transmission all the collisions will be detected. Now let us come to the second important standard that is your IEEE 802.4 based on token bus.

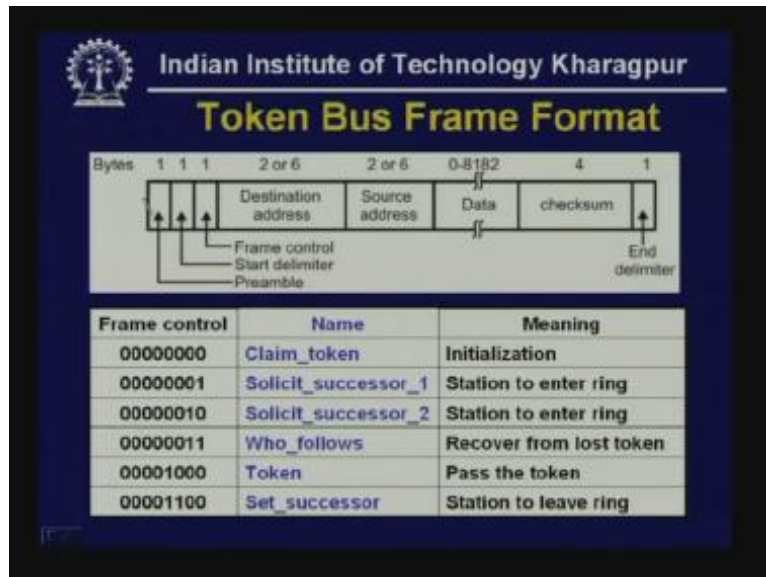
(Refer Slide Time: 38:45)



Because of the non deterministic nature of the medium access control that is CSMA/CD many people from industry were not satisfied with the CSMA/CD protocol that is your 802.3, particularly general motors who are interested in factory automation. They suggested there should be an alternative where we can send real-time traffic or the time is deterministic that is the maximum delay is deterministic and that's how the token bus standard was developed by IEEE 802 committee. Here (Refer Slide Time: 38:16) as usual like Ethernet or IEEE 802.3 a bus is used and in two ways the computers are connected, the way the computers can be connected in IEEE 803. However, they form some kind of a logical ring as you can see. A is connected to B, and B is connected to E, and E is connected to G but it is not necessary that they will follow the same order. So the order in which it is connected to the cable can be different from the order in which this logical ring is formed.

Then each station passes a token to its successor to gain access control of the bus. That means there is a token, each station will get a token and whenever it gets a token it transmits the data and in this way the data transmission is possible. And there are four priority classes 0, 2, 4 and 6 with 0 as the lowest and 6 as the highest priority. That means if a particular station has frames of highest priority it will first send those frames and then other station then it will send the lower priority station. So we find that to support real time traffic priority concept is introduced in token bus protocol. And here is the frame format used in token bus standard.

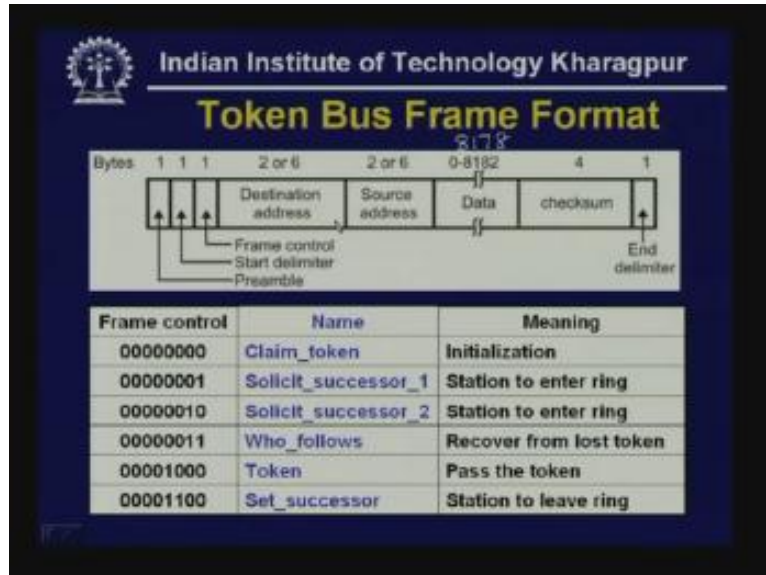
(Refer Slide Time: 39:57)



As you can see this frame format is different from IEEE 802.3 frame. Here you have got the preamble. Preamble is essentially for the purpose of synchronization. But instead of seven bytes here it is only one byte, then there is a start delimiter which signifies the beginning of the frame and also there is an end delimiter which is a special character used for marking the start and end of the frame.

The packet length is not mentioned here and this is essentially limited by the start delimiter and end delimiter. And as usual there are destination address and source address. However, the token bus standard allows 2 byte or 6 byte address and 6 byte address is very similar to that IEEE 802.3. Then the data size can be here from 028182. Of course whenever 6 byte address is used you have to subtract 4 from here so it becomes 028178. It is the maximum whenever 6 byte address is used. Whenever 2 byte address is used then it is 028182.

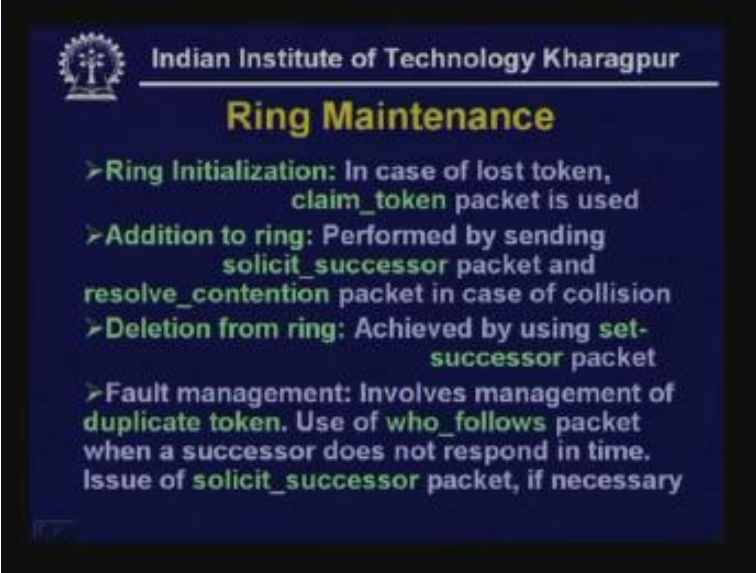
(Refer Slide Time: 41:20)



Now, there is a frame control bit, the frame control bit has got the priority bits and it signifies whether it is a data frame or a token or a control frame and it performs various types of control, apart from priority it is a control frame. As you can see there are several types of frame controls which are mentioned here such as claim token, solicit\_successor\_1, solicit\_successor\_2, who\_follows, token, and set\_successor. Let us see how it is being done in a distributed manner in token bus which means ring maintenance.

Ring maintenance is a very complex case in case of token ring. Possibly the medium access control is the most complex here. As shown here this claim token packet is used in the beginning at the time of initialization in case of a lost token, or whenever there is no token at all. That means when a particular station is turned on, a system is turned on then it will send a claim token packet and it will say that this particular station is holding the token. That means in the beginning there will be no station active so whenever a particular station turns on it sends the claim token packet and it sends the token, it essentially is the holder of the token.

(Refer Slide Time: 43:30)



Indian Institute of Technology Kharagpur

## Ring Maintenance

- > **Ring Initialization:** In case of lost token, **claim\_token** packet is used
- > **Addition to ring:** Performed by sending **solicit\_successor** packet and **resolve\_contention** packet in case of collision
- > **Deletion from ring:** Achieved by using **set-successor** packet
- > **Fault management:** Involves management of **duplicate token**. Use of **who\_follows** packet when a successor does not respond in time. Issue of **solicit\_successor** packet, if necessary

Now, one after the other the stations have to join the ring, how it can be done? That is done with the help of this **solicit\_successor\_1** frame. Whoever is holding the token occasionally will send this **solicit\_successor\_1** frame. So, whenever a **solicit\_successor** frame is sent the other stations waiting for joining the ring will respond and join the ring.

However, if there is collision there is a possibility that more than one station are waiting and are wanting to join the ring then the **resolve\_contention** packets are used to resolve the collision. In this way one after the other rings can join.

Suppose a particular station has the predecessor P and successor S, this is the address, that means if a new station joins then the new station's will be the successors address so it's a new address and the new station will have X as the predecessor and the successor will become the address of the new station. So in this way a station can join.

(Refer Slide Time: 44:40)

Indian Institute of Technology Kharagpur

## Ring Maintenance

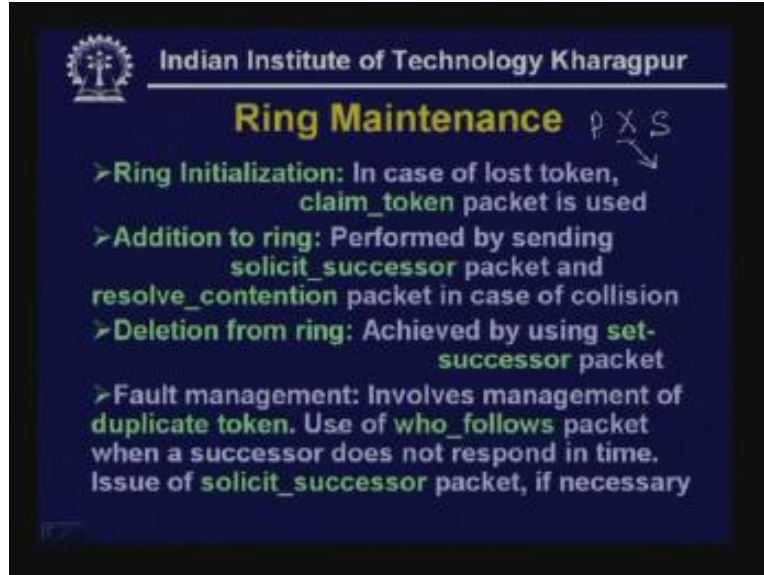
- > Ring Initialization: In case of lost token, **claim\_token** packet is used PXS
- > Addition to ring: Performed by sending **solicit\_successor** packet and **resolve\_contention** packet in case of collision
- > Deletion from ring: Achieved by using **set-successor** packet
- > Fault management: Involves management of **duplicate token**. Use of **who\_follows** packet when a successor does not respond in time. Issue of **solicit\_successor** packet, if necessary

However, the addresses are arranged in a descending order. That means the packets are transmitted in a descending order. that means here it goes from the highest address to the lowest address and so on, in this way it goes (Refer Slide Time: 45:09). Then a particular station may want to leave the ring in that case it sends a `set_successor` packet. It is very easy to do.

For example, a station has the predecessor P and a successor S and if it wants to leave the ring it will simply ask the predecessor to make X as its successor. So now X is the successor of P but now X will request so X as a successor of P in this way X will come out of the ring. This is done by using the set successor packet by sending this particular this successor's address.



(Refer Slide Time: 46:10)



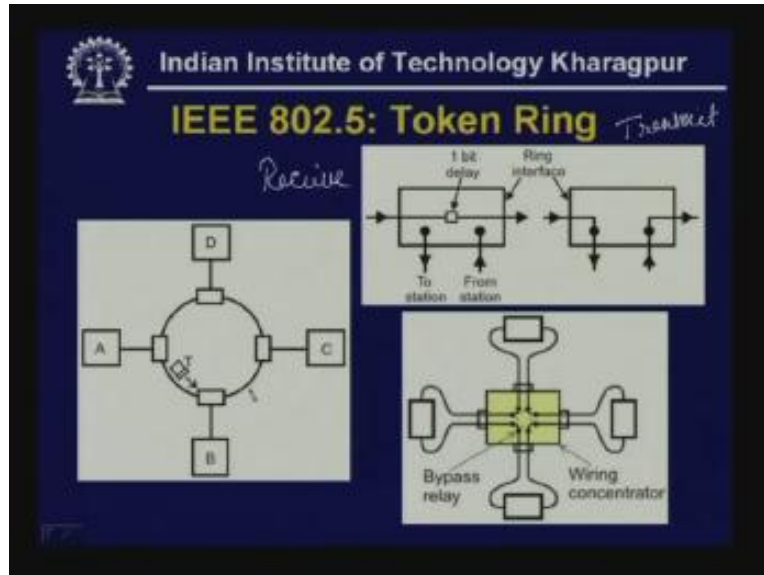
Solicit\_successor\_2 is also necessary in situations where, suppose there is no response from other stations in that case this is being used for new stations to join the ring. Now this fault management is necessary, involves management of duplicate frame so it uses who\_follows packet when a successor does not respond in time. that means in this case what is happening is a particular station has sent a token, its successor either should send the data frame or it should send the token but if does not respond then this is being done and who\_follows packet is sent.

Who\_follows means the next successor, that is, if the successor does not respond then the successor of the successor has to respond. If the successor of the successor does not respond then this particular solicit\_ successor\_2 is introduced so that whoever is in the ring waiting for joining can join.

In this way the ring maintenance is being done in a dynamic manner. So here we find this ring maintenance is performed in a distributed manner and any station that is holding the token will act as some kind of a master and issue these control frames. On the other hand, in IEEE 802.5 which is based on token ring the rings are organized in a logical way, physical way.

As you can see, here it can operate in two modes. Either it is in the received mode or monitor mode or in transmitter mode. So, if a particular station is simply looking at or watching the frames to go by then it receives the packet it intrudes a delay of one bit and then returns message. So in this way there is a delay of one bit as a token or a frame goes by. But if a particular station gets a free token then it grabs it then it changes to the transmit mode. So whenever it changes to the transmit mode it breaks the link as you can see logically (refer Slide Time: 49:05) and it receives the token then it transmits the frame into the ring.

(Refer Slide Time: 49:12)



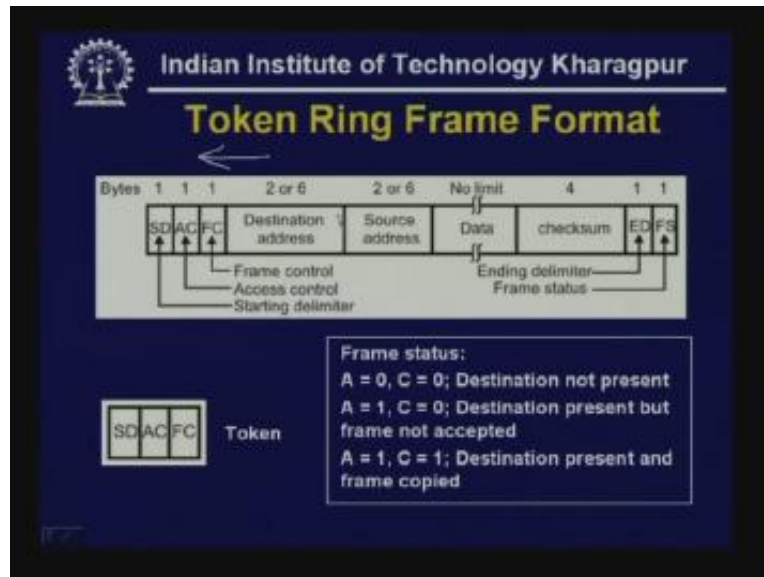
This is how there are two possible modes. One is the received mode, another is transmit mode. Now this is a very unreliable situation in the sense that the way it is being connected. If there is a break anywhere then the entire ring collapses, no communication is possible because each particular station has to take part in relaying the token or the frame. So, to overcome that problem a wiring concentrator is used where all the cables are connected to a central point which acts as some kind of central node, this wiring concentrator, and there is a bypass relay for each of these stations.

So whenever a particular station becomes faulty then it can be bypassed by closing a micro switch or relay for each of these stations. We can call this a third mode known as 'bypass mode' whenever this kind of wiring constructor is used. So, in this topology the reliability of the topology can be improved by introducing a wiring constructor as you can see.

Now here is the token ring frame format and as you can see there are three bytes. first one is the starting delimiter, second one is the access control and third one is the frame control and then you have got the destination address, sources address as usual, it can be from two to six bytes. And surprisingly there is no limit on the data size in case of token ring network, it uses only four byte checksum for error detection and there is an ending delimiter and there is another byte at the end which essentially is used to indicate the frame status.

That means as the frame goes by obviously it is going in this direction (Refer Slide Time: 51:22). first the starting delimiter, then access control, then the frame control, then the destination address, source address, data etc so in this way goes and at the end when the last byte goes by the frame status can be indicated with the help of two bits A and C bits.

(Refer Slide Time: 51:45)



Thus, if the destination is not present that means by looking at this address (Refer Slide Time: 51:50) if it comes back then both are 0 0, initially these two bits are 0 0 then as the ring covers them, if your destination address gets it but if there is error then it does not accept the packet so it changes the bit A to 1 but C remains to 0, then as the frame goes by if it finds that the checksum is also correct then it sets both the bits A and C bits to 1.

So, in this case destination is present and frame is copied. That means as the frame goes by automatically the frame status bit senses and it acts as an acknowledgment to the source address. So when the frame goes to the destination it removes it and not only it removes but it comes to know whether there is an error or the frame has been removed and so on.

As you can see there is a token, whenever there is no data then there is no need for destination address, source address or anything so the access control bit specifies that this is a token and token is only three bytes comprising starting delimiter, access control and frame control. That means whenever there is no data this token keeps on circulating. In a lightly loaded token ring network most of the time the token will keep on circulating. However, whenever a station has some data we will **grab** the frame and it will convert the token into this kind of frame format and signal.

Now there is a monitor. One of the stations is designated as a monitor station which performs the ring maintenance. Particularly it does duplicate address test, it does fault location whenever there is some break in the network and whenever it finds that there is no monitor it tries to claim the **token to become a monitor this is necessary in the beginning**, and whenever there is a power frame packet circulating around the ring it purges and also occasionally it sends a token frame indicating that the active monitor is present and also there are some other stations that possess the potential to become a

monitor so occasionally it sends this kind of frame so that when the monitor fails then particular standby monitor will take over.

(Refer Slide Time: 54:45)

Indian Institute of Technology Kharagpur

### Ring Maintenance

➤ Each token ring has a monitor station

Frame control	Name	Meaning
00000000	Duplicate address test	Same address test
00000010	Beacon	Fault location
00000011	Claim token	Attempt to become monitor
00000100	Purge	Reinitialize the ring
00000101	Active monitor present	Issued periodically by the monitor
00000110	Standby monitor present	Presence of potential monitors

Here is a quick comparison of the three protocols. So far as the access determination is concerned CSMA/CD uses contention, token bus uses a token, token ring also uses a token passing.

(Refer Slide Time: 55:10)

Indian Institute of Technology Kharagpur

### Comparison of 802.3, 802.4 and 802.5

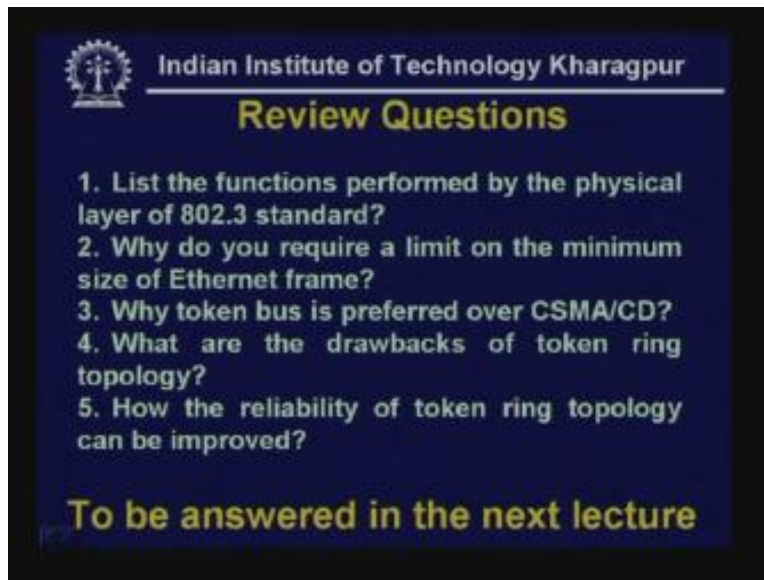
Function	CSMA/CD	Token bus	Token ring
Access determination	Contention	Token	Token
Packet length restriction	64 bytes (Greater than $2 \times T_{prop}$ )	None	None
Priority	Not supported	Supported	Supported
Sensitivity to work load	Most sensitive	Sensitive	Least sensitive
Principle advantage	Simplicity, wide installed base	Regulated/fair access	Regulated/fair access
Principle disadvantage	Nondeterministic delay	Complexity	Complexity

In case of CSMA/CD there is a packet length restriction of 64 bytes which has to be greater than twice the maximum propagation time. In case of token bus or token ring

there is no such limits. Then priority is not supported in CSMA/CD, it is both supported in token bus and token ring and as sensitivity to work load is concerned this CSMA/CD is the most sensitive, token ring is sensitive but token ring is the least sensitive. And the principle advantage of CSMA/CD is the simplicity and it has got wide installed base.

Token bus has got regulated or fair access. The token ring has also got regulated and fair access. The principle disadvantage of CSMA/CD as we know is the non deterministic delay and token bus has the highest complexity and token ring is also complex but lesser than the token bus. So here is the time to give you the review questions.

(Refer Slide Time: 56:15)



Indian Institute of Technology Kharagpur

### Review Questions

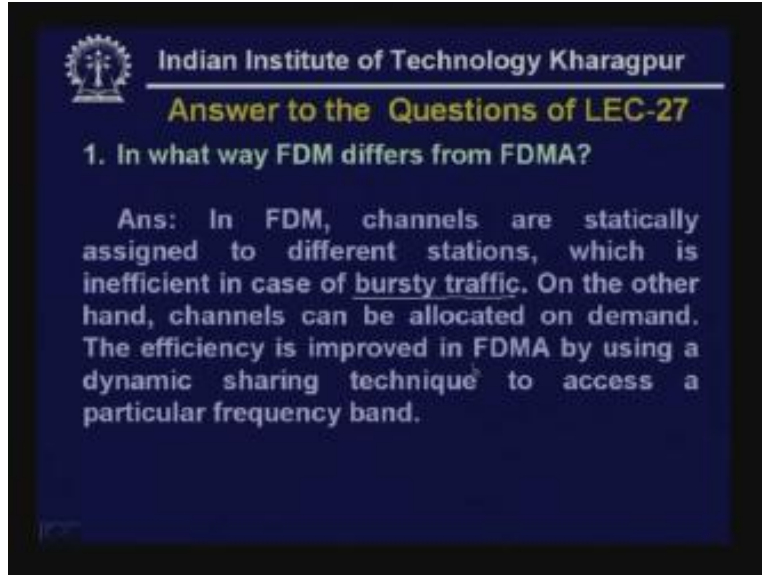
1. List the functions performed by the physical layer of 802.3 standard?
2. Why do you require a limit on the minimum size of Ethernet frame?
3. Why token bus is preferred over CSMA/CD?
4. What are the drawbacks of token ring topology?
5. How the reliability of token ring topology can be improved?

To be answered in the next lecture

- 1) List the functions performed by the physical layer of 802.3 standard?
- 2) Why do you require a limit on the minimum size of Ethernet Frame?
- 3) Why token bus is preferred over CSMA/CD?
- 4) What are the drawbacks of token ring topology?
- 5) How the reliability of token ring topology can be improved?

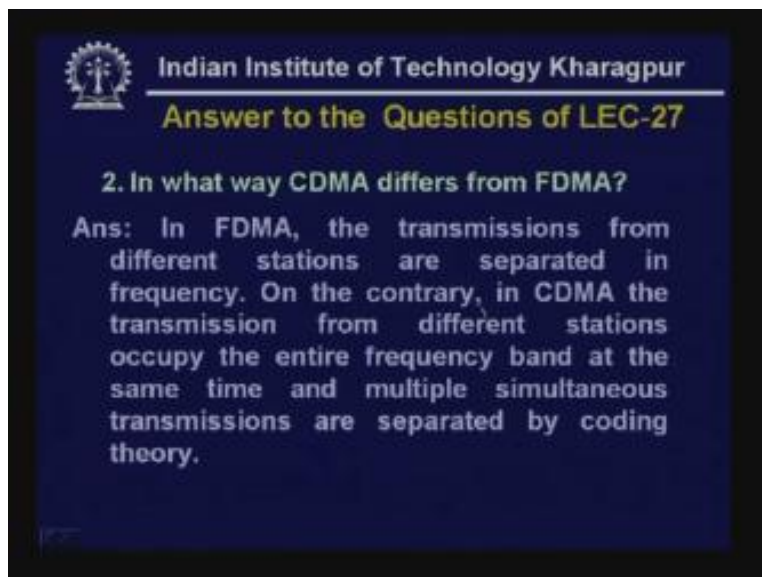
These questions will be answered in the next lecture. Here is the answer to the first question of lecture minus 27.

(Refer Slide Time: 57:00)



1) In what way FDM differs from FDMA?

In FDM channels are statically assigned to different stations which is inefficient in case of bursty traffic. On the other hand, channels can be allocated on demand. The efficiency is improved in FDMA by allocating on demand by using dynamic sharing technique to access a particular frequency band. So this is your FDMA.

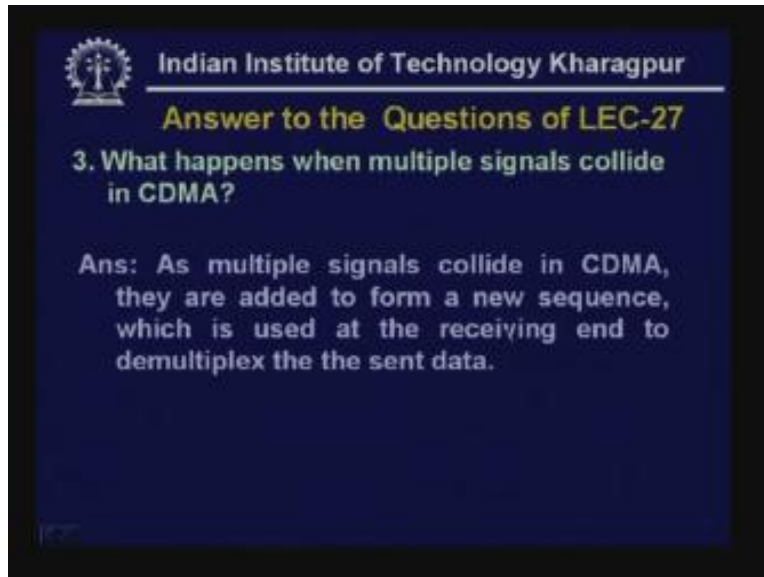


2) In what way CDMA differs from FDMA?

In FDMA the transmissions from different stations are separated in frequency.

On the contrary in CDMA the transmission from different stations occupy the entire frequency band at the same time and multiple simultaneous transmissions are separated by coding theory.

(Refer Slide Time: 57:35)



3) What happens when multiple signals collide in CDMA?

We know that as multiple signals collide in CDMA they are added to form a new sequence which is used at the receiving end to demultiplex the sent data.

What is an inner product?

It is essentially two code sequences are multiplied element by element and the result is added we get a number called inner product. For example,  $S_1$  and  $S_2$  are two codes and if we multiply them and add them we get 0. So, if you multiply two different inputs we get the inner product as 0. On the other hand,  $S_1$  into  $S_1$  is equal to 4 because you have got four chip sequences, so inner product is 4.

(Refer Slide Time: 58:34)

Indian Institute of Technology Kharagpur  
Answer to the Questions of LEC-27

4. What is an inner product?  
Ans: If two code sequences are multiplied, element by element, and the results are added, we get a number called inner product.

➤ Example: Let there are two code sequences  $S_1 = \{+1, -1, +1, -1\}$  and  $S_2 = \{+1, +1, -1, -1\}$ . Now  $S_1 \cdot S_2 = +1 -1 -1 +1 = 0$ . So, the inner product is 0. On the other hand  $S_1 \cdot S_1 = +1 +1 +1 +1 = 4$ . So inner product is 4. Similarly, the inner product for  $S_1 \cdot \bar{S}_1$  is 0.

Similarly, the inner product for  $S_1$  into  $\bar{S}_1$  is equal to 0, also it can be  $S_1 \cdot \bar{S}_2$  is equal to 0.

(Refer Slide Time: 58:44)

Indian Institute of Technology Kharagpur  
Answer to the Questions of LEC-27

5. Compare and contrast FDMA, TDMA and CDMA techniques.  
Ans: In case of FDMA the bandwidth is divided into separate frequency bands. In case of TDMA the bandwidth is timeshared. On the other hand in case of CDMA data from all stations are transmitted simultaneously and are separated based on coding theory. Unlike FDMA, CDMA has soft capacity, which means that there is no hard limit on the number of users. Capacity of FDMA and TDMA is bandwidth limited, whereas the bandwidth of CDMA is interference limited. CDMA offers high capacity in comparison to FDMA and TDMA. CDMA also help to combat multipath fading.

4) Compare and contrast FDMA, TDMA and CDMA techniques.

In case of FDMA the bandwidth is divided into separate frequency bands, in case of TDMA the bandwidth is timeshared, on the other hand, in case of CDMA data from all stations are transmitted simultaneously and are separated based on coding theory. Unlike FDMA, CDMA has got soft capacity which means that there is no hard limit. Particularly



in FDMA and TDMA it is band limited. On the other hand, in CDMA it is interference limited. But CDMA offers high capacity in comparison to FDMA and TDMA. CDMA also helps to combat multipath fading.

With this we conclude today's lecture. In the next lecture we shall discuss about high speed local area networks, thank you.