Computer Networks and Internet Protocol
Prof. Soumya Kanti Ghosh
Departments of Computer Science and Engineering
Indian Institute of Technology Kharagpur

Lecture – 47
Data Link Layer-Basic Concepts

Hello. So, we will be continuing our discussion on Computer Network and Internet Protocol. So, we have started discussion on Data Link Layer. So, overview of the things we will again look at some of the basic concepts and then we will go slowly to little bit specific things which we want to discuss, right.

So, as we have discussed in our earlier lecture that data link layer is a layer 2 position of OSI and also the TCP IP protocol stack. It plays important role because finally, the for transmitting any data that data link layer address need to be resolved, right. And finally, and end of the things we require a physical media wired or wireless to transmit the data from one source to another from the source to destination or hub to hub. Or data link layer manifestation sometimes we call is a hub to hub manifestation, right.

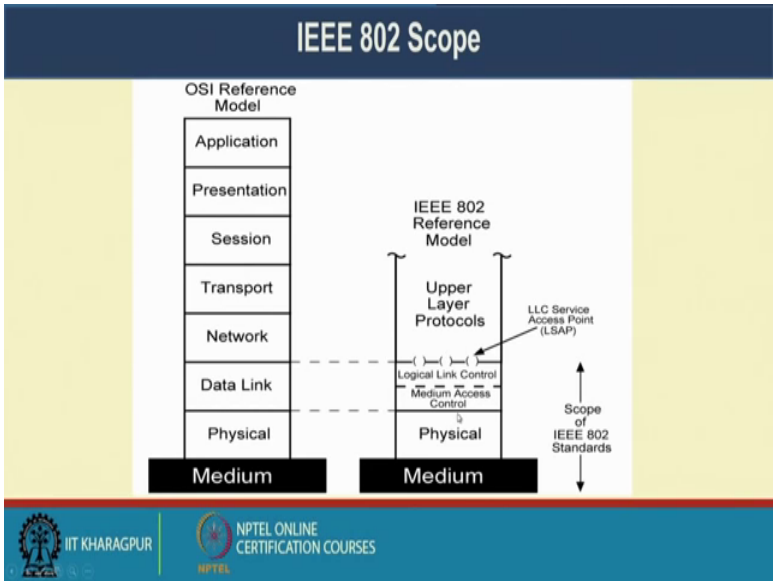
So, this is important to understand the different fill means different functionalities or mechanisms of data link layer. Though whenever we are writing as a application network application, writing an application or working as a network admin not primarily for application etcetera may not be much always bothered about the data link layer, we are mostly at the higher layer protocols and type of things. But to understand things it may help us in optimising at different level.

And these days as we have seen that lot of cross layer issues are coming up or cross layer optimisation challenges are coming up, lot of research going on, cross layer optimisations which taking care that not that individually things but taking the stack or a portion of the stack together that it is important to understand, right. Because our all protocol things were primarily why we made stack because that one layer should work independently and it should only bothered about its upper layer and the down layer, right.

So, this, it is extremely nice or for interoperability between different devices, different protocols and type of things, but in doing so, more you make it flexible more you lose on performance or maybe there is a compromisation of the performance; so that there is

people looking at the cross layer optimisation. In some of the cases like quality of service or even type of services, security, overall network management etcetera this called cross layer things optimisation things come up and several applications made demand a not only one layer but a optimised different layer, type of things maybe multimedia application or some secured application over the things etcetera. So, those things are some of the aspects which we look into this in case of a your data link layer (Refer Time: 03:33) that aspects is important to understand that why things are there, right.

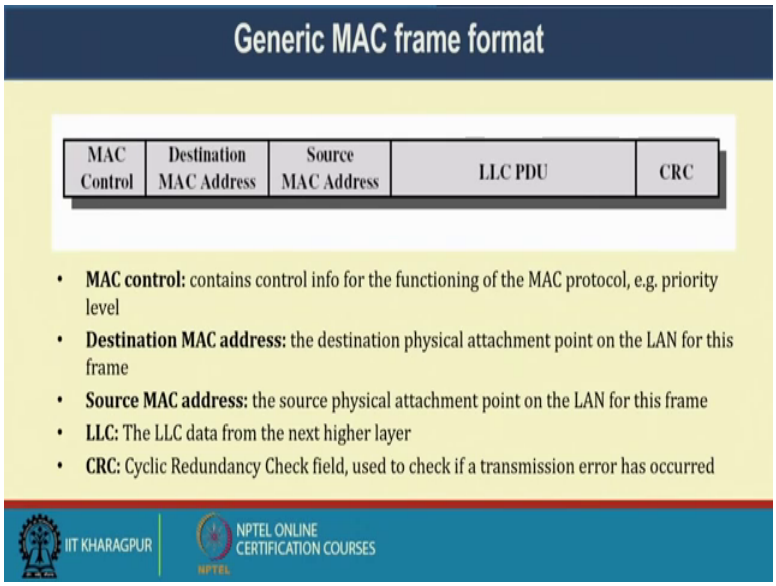
(Refer Slide Time: 03:59)



So, just to recap what with one slide what we have seen that data link layer is primarily consist of two things, one is LLC or Logical Link Control, another in the medium access control. So, LLC is primarily responsible for upper layer negotiation or upper layer connectivity etcetera, whereas the MAC is primarily with the physical layer, right.

So, LLCs as LSAP or the LLC service access point and on other sense that MAC also have a MAC address, sometimes we call a hardware address type of hardware address those are at the MAC level, right. And if you look at the I triple E 8 naught 2 standard, it encompasses both these layer 2 and the physical layer stuff.

(Refer Slide Time: 04:31)



Now, if you look at the generic MAC frame format, right. So, MAC layer it forms a frame. So, what is the MAC frame format? Its payload is the LLC PDU, right protocol data unit which it gets from the LLC as its payload and it addresses the source MAC address and destination MAC address and there are some control MAC control is at the front of it. At the end it gives the CRC or the redundancy check field to find out whether there is a transmission error or not by the end station or the next stop station where the things are being transmitted, right. So, that is important.

So, we have a MAC control, contains the control information of the function of the MAC protocol that is priority level, etcetera. Destination MAC addresses; the address of the physical attachment point of the LAN for this frame, right; so where it is connected, right. So, your number of cases if the; if your PC or laptop say watt connection connected to a switch, so that is the destination for this, the next stop is the switch, right. And if it is a wireless then also the destination is the wireless access point is for it (Refer Time: 05:54) hub to hub things, right and there is source MAC address, the source physical attachment point of the LAN of this things.

So, attachment point means where it is connecting to network interface cut. So, that is important. So, what another is the LLC; the LLC data from the next higher layer, right. So, the whatever the data it gets from the next higher layer is the LLC PDU things are there and CRC is the redundancy cycling redundancy check field used to check if the

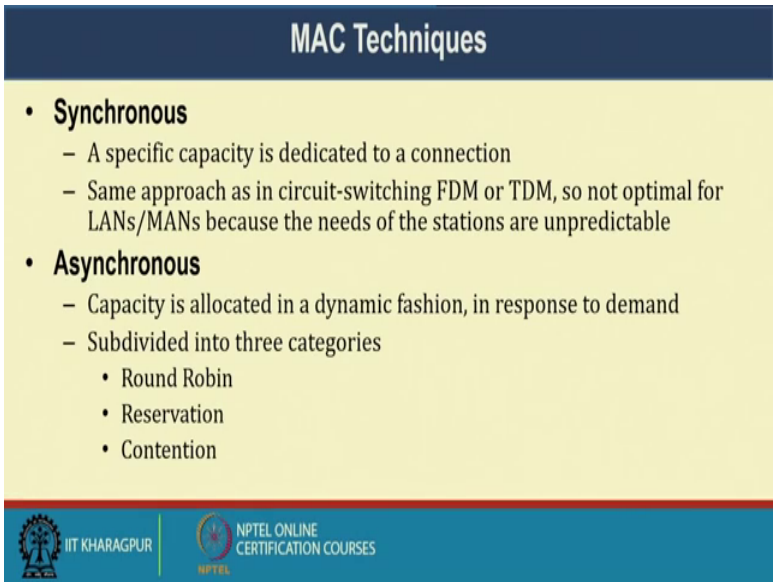
transmission error has occurred or not. Set the distance and check whether the CRC checking is there, right. So, we will see that if we can discuss on the CRC prime permits in some later lectures, but otherwise you can refer any standard book.

Now, important is that that I have a frame which is on the standard and as we understand that the for this we require a physical device network adaptor card or what we say LAN card where you have you can plug in your vat, RJ 45 type of cable. Or if it is a wireless antenna or that trans receiver things will should be there or if it is a something other things like some other things, (Refer Time: 07:26) things those inter phases will be there, that card fits into over devices it is laptop, PC, server whatever, right. And it contains a physical address, right. Physical address or MAC address or hardware address sometimes. So, it comes with manufacture things. So, it comes with the address which is embedded into the things, right. So, that is important.

Though there are things we talk about cloning of MAC address etcetera, we are not going to those issues or complicacies as of now this MAC address is unique. That means, any device having a interface card has a unique MAC address across the world, right. So, what we required to do? We need to have a logical connection between the source and destination from the IP address then every hub it needs to know that, what is the next IP address, dissolve the MAC address push it to this MAC into this MAC.

Because the layer 2 only understands up to the layer 2 things that means, up to MAC layer LLC layer it understand. Layer 2 does not understand IP etcetera, right because there is a higher level things. So, that need to be addressed need to be resolved need to be resolved as by some protocol, we know there is the protocol called ARP, Address Resolution Protocol with allows this which maps this IP address to this MAC address, right and then goes on doing those things.

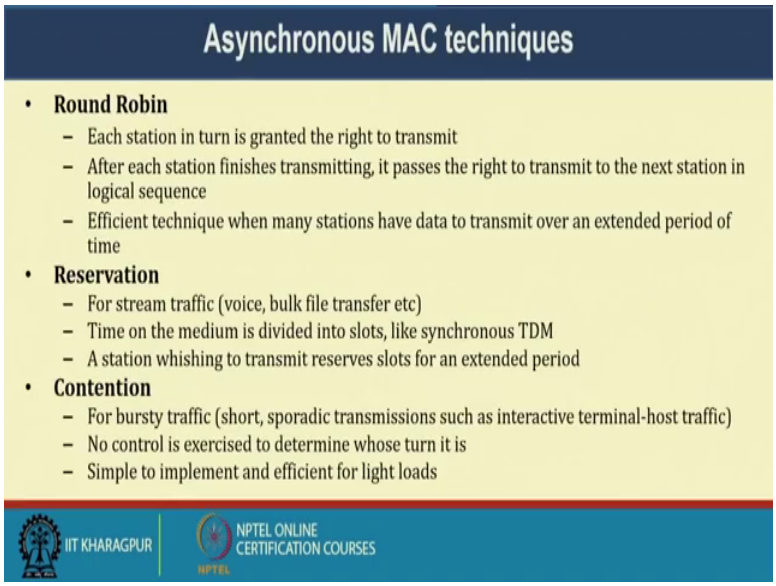
(Refer Slide Time: 08:57)



Now, MAC techniques or MAC approaches can be one is synchronous, a specific capacities dedicated to a connection. Same approach as in circuit switch FDM that is or TDM that is frequency domain multiplexing or time domain multiplexing. So, not optimal for the land or metropolitan area network because the need of the station may be unpredictable, right. So, you can synchronous and reserved things may not be dedicated connection may be very appropriate. On the other way we have the asynchronous, capacities allocate dynamically dynamic fashion in response to the demand.

When the demand comes, it is the capacities allocated. Subdivided or you can see that we can have with it 3 approaches, one is Round Robin, I go on getting things after every particular time slot. It can be some reservation strategy it is reserved for the things or there can be contention, right I contain for that slot and get the things done.

(Refer Slide Time: 09:59)



So, round robin, in case of a round robin for asynchronous MAC techniques, which more predominant, MAC synchronous things. So, in case of Round robin what we say that each station is in turn granted right to transmit, right. So, it is not that it is fixed, so each station gets its turn to write to transmit after each station finish in transmitting it passes the, right to transmit to the next station in the logical sequence, right. So, once transmission there it goes to the next.

Efficient technique when many stations have data to transmit over an extended period of time. If the everybody is wants to transmit it is efficient, right but if there are station which are nothing to transmit then also it is getting a turn and it is a wastage of the things, right. So, it is it becomes efficient when everybody wants to transmit or the data are more or less in uniform manner we want to transmit and type of things it becomes much easier, very much efficient, otherwise it will be loss of things like, it goes on getting turns but nothing transmitted.

Whereas, in the in case of a reservation for it is more appropriate for some of the traffic where like stream traffic like voice, bulk file transfer etcetera. Time on the medium is divided into slot like synchronous TDM, a station wishing to transmit reserve the slot for extended period. So, it is it has a it in case of steady (Refer Time: 11:34) traffic you have a quit a volume of data to be transmitted, so you reserve the slot to be transmitted, right a priori before transmitting, right.

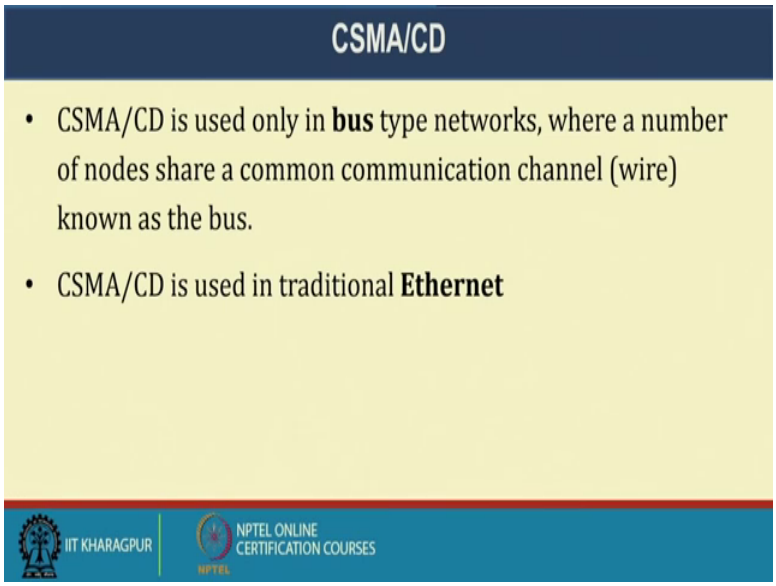
And the third one which is contenders contents contention based technique that is for bursty traffic, short, sporadic transmission such as interactive terminal host traffic and type of things which is which are predominant in case of a normal network traffic. No control is excised on to determine whose turn it is, right. So, there is no control on the thing simply to implement then efficient for light load. So, it is it is something contention. A content for that slot and get the things and it is something which is very means what we say simple or out of the (Refer Time: 12:31) simple to implement and efficient for light load. So, if it is a heavy load and traffic etcetera need to be transmitted. So, that may be a problem otherwise it is efficient.

(Refer Slide Time: 12:43)

So, if you look again in the medium access method, so there are two things which is predominant, one is Carrier Sense Multiple Access with Collision Detection CSMA CD for bass topologies which are which we mostly see across us, right CSMACD.

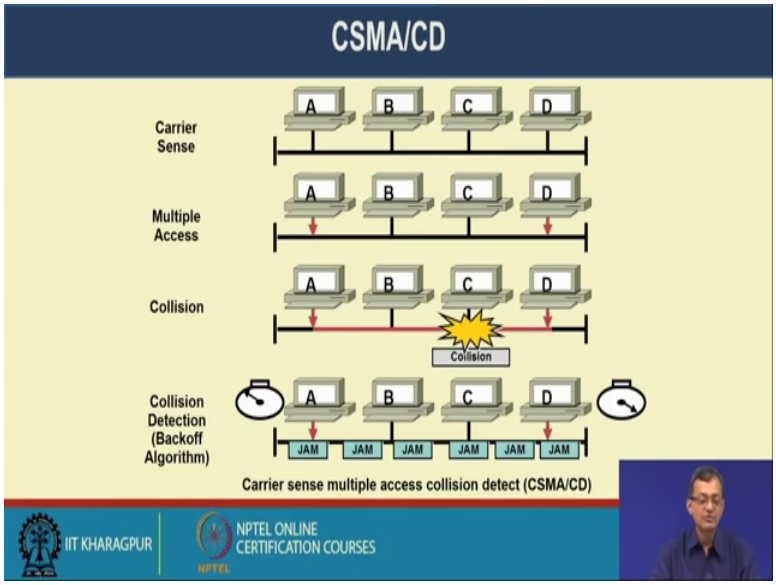
There is another thing which is still there but not so popular that is control token or token passing for bus and ring topologies, right. So, this is also there, but not so popular these days. So, we are mostly on CSMACD type of architecture.

(Refer Slide Time: 13:23)



So, in case of a CSMACD used only in bus type of network where a number of nodes CRA common communication path or bus or what we say communication media, right. So, I have a communication path where the number of nodes or number of systems or end system transmit through that bus, that it is the it is also the technique in our traditional Ethernet connectivity, right CSMACD is the technique.

(Refer Slide Time: 13:57)

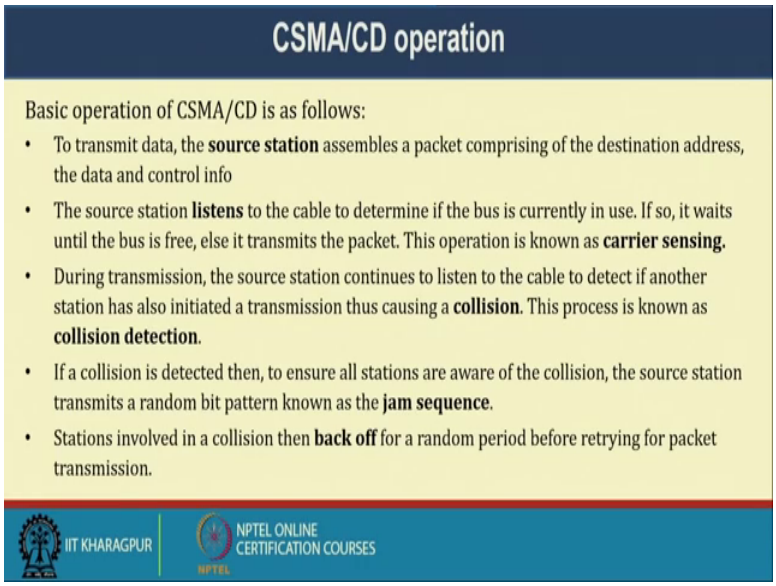


So, what we say that it need to carrier sense it need to sense whether there is a channel is free or not. So, there is a whether the carrier is free or not it tends to sense. There is a

question of multiple access that number of thing can access at the same time, there is a phenomenon of collision that party communicate and may collide, right and there is a that should be a way to detect the collision and there should be a back of algorithm. So, once collision is there that should be a back off and retransmission, so need to be jammed that there is a collision is occurred that do not transmit and there is a back off algorithm so after some time there should be a retransmission, right.

So, one is that I need to sense it, one definitely there is a multiple access I need to sense it and if in spite of that there is a collision there should be a way to handle this collision and retransmit the data in a using some back off algorithm.

(Refer Slide Time: 15:05)



So, if you look at the basic operation to transmit data the source station assembles a packet comprise of the destination address and that data and the control info at the layer two level. The source station listen to the cable or the transmission media to determine if the bus is currently is in use or not, if so it waits until the bus is free else transmit else it transmit the packet, right.

So, if there is free transmit if it is not free it waits whether the bus is free and transmit the operation is known as the carrier sensing. So, if it carrier sense if it is not free it wait for the time and if it is free transmit. During the transmission the source station continues to the listens to the cable or the media to detect if another station is also initiated transmission that causing a collision. So, it look at the collision things.

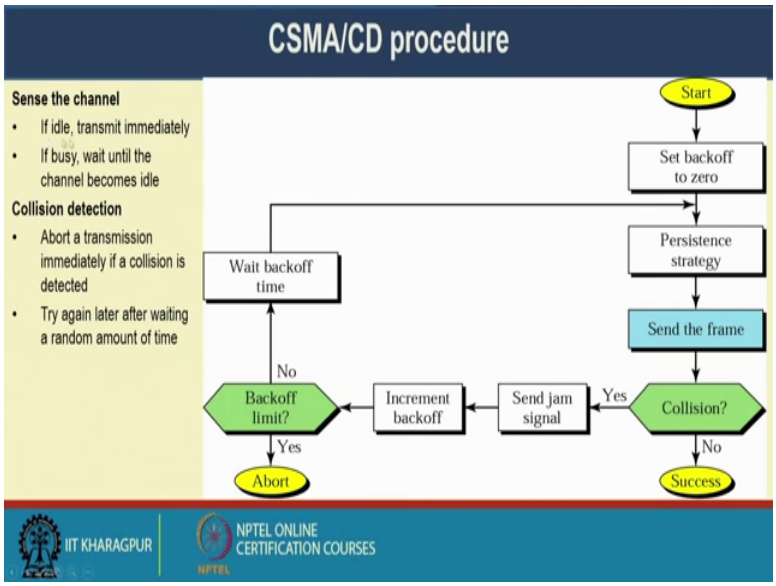
So, collision and this process is a collision detection. Typically there is a if there is a collision there is a fluctuation in the voltage level etcetera which it the source station hardware suit able to capture that and there is a what we say collision detection. If a collision has detected then to ensure all station are aware of the collision the source station transmitted random bit pattern known as jam sequence, right. So, if the collision is detection detected then other station will may also jumped in to the thing, right without knowing that collision is there and it will be more collision and things will be there. So, what it does source station that it sends a jam signal. So, random bit pattern which is (Refer Time: 16:45) jam signal.

The station involved in a collision then back off for a random period before retrying the packet for the transmission. So, the whichever station involved in this in a this collision scenario will then back off for a random time period before retrying for transmitting the packet, right. So, that is the fundamental way (Refer Time: 17:13).

So, let me just repeat the thing the it assembles first off all source station assemble the packets or it forms that MAC level frame. And then look listens to the media if there is media is free it transmit, if the media so this the carrier sensing, if it is not free it I need to wait if it is once transmission if there is a collision usually detected by the fluctuation of the voltage the source station go for a collision detection mechanisms. If the collision is detected or collision has occurred then the source station send a random beam pattern or a jam signal jam sequence to alert other station that there is a collision has occurred, right.

And on listening that the stations which are preparing for involved in this collision or preparing to transmit it will wait for a random back off time we will see that how things are there in the protocol thing. So, it is basically back off time before retransmitting or checking the again going to the loop checking the station and going on to the transmitting the data.

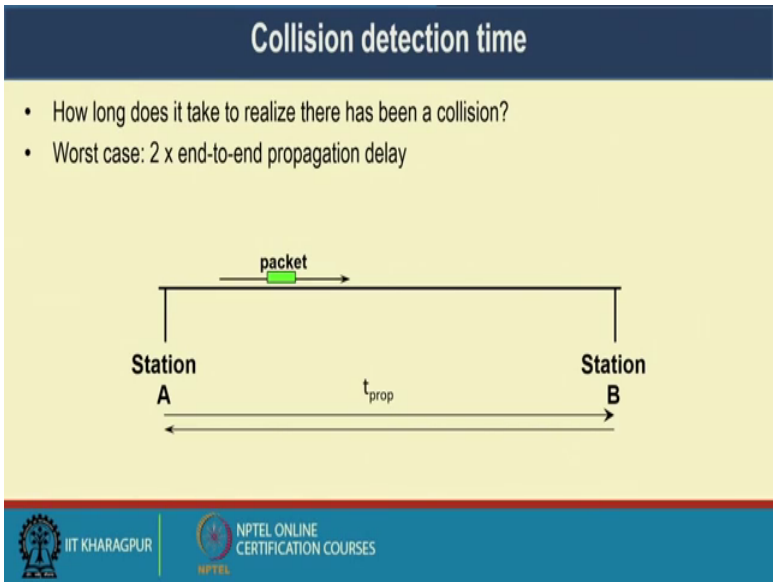
(Refer Slide Time: 18:33)



The same thing, so sensing if the idle transmit immediately if busy wait till the channel becomes idle collision detection abort a transmission immediately if the collision is detected, try again later after waiting a random amount of time, right. So, if we look at the sequence start then set back off to 0, if it is a persistence strategy check that the what sort of persistence strategy is there, send the frame, if there is a collision no then it is a success, if this is a so transmission is there if there is a collision send jam signal in that land segment then there is increment the back off time. And if the back off limit has not crossed then wait for the back off time and then retransmit, right.

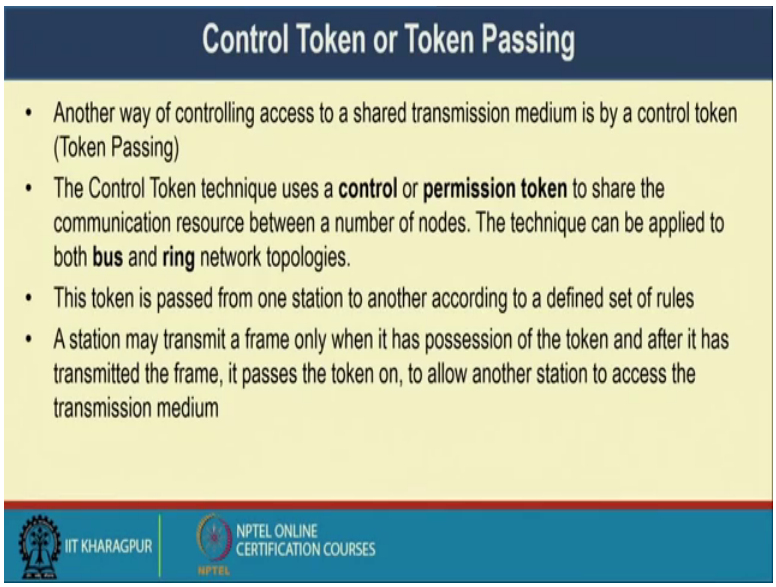
The same thing if the limit has cross then just abort the thing, right that how much time you can go on trying there if the limit has crossed then you say that you about the connection or say that there is transmission link failure or something is not there. So, this is the way it works in case of this, when we transmit the things in a collision detection in a multiple access carrier sense multiple access with collision detection CSMACD.

(Refer Slide Time: 20:05)



Now, when collision detection time how long does it take to realise that there is a collision? The worst case it may happen that to cross end to end propagation delay, right. So, it is a end to end propagation delay twice that I think then we can have this whether there is a collision has occurred or not. So, that maybe the scenario which will be there, right.

(Refer Slide Time: 20:29)



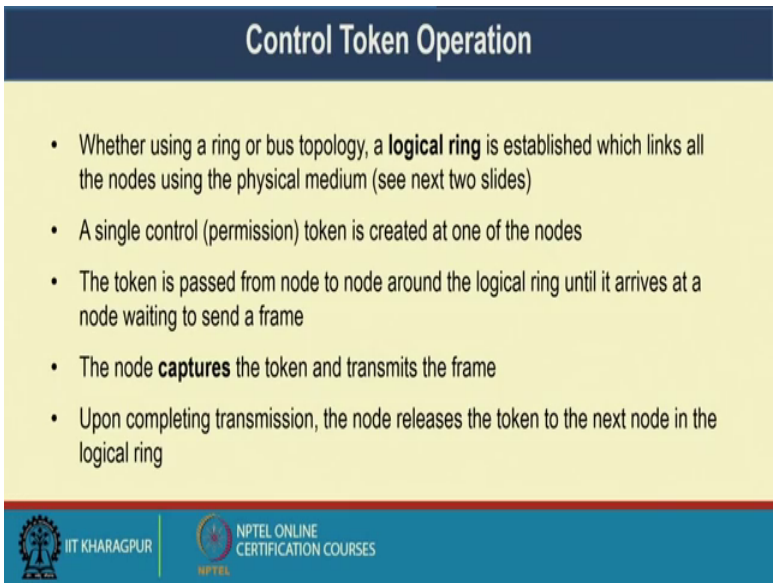
So, there is a another protocol what we have just mention at the beginning which is which is still they are but not so predominal but just to have a overview of this sort of a

MAC level protocol. So, this control token or token passing another way of controlling access to the CR media is by control token or token passing so that means, whoever the in the control of that token has, right to transmit, right.

The control token technique uses a control or permission token to say at the communication resource between the number of nodes, right. This technique can be applied to both bus and ring topologies. So, this control token thing this token is passed from one station to another according to a defined set of rules. So, that how this thing should passed or shared it is a defined into the thing.

So, a station may transmit a frame only when it possess a token that means, you have a control of the token or token is in your hand then only the station can transmit the frame. And after it has transmitted the frame it passes the token on to allow another station to grab that token and in turn used at media to transmit that data, right. So, this is the basic philosophy which it works. So, in other sense we have a tokenization mechanism or a what we say control or permission token the station which has the control about the token or has the token in its hand has the way to transmit after transmission it pass the token on so that the other contending stations who wants to transmit can use this token to transmit.

(Refer Slide Time: 22:19)

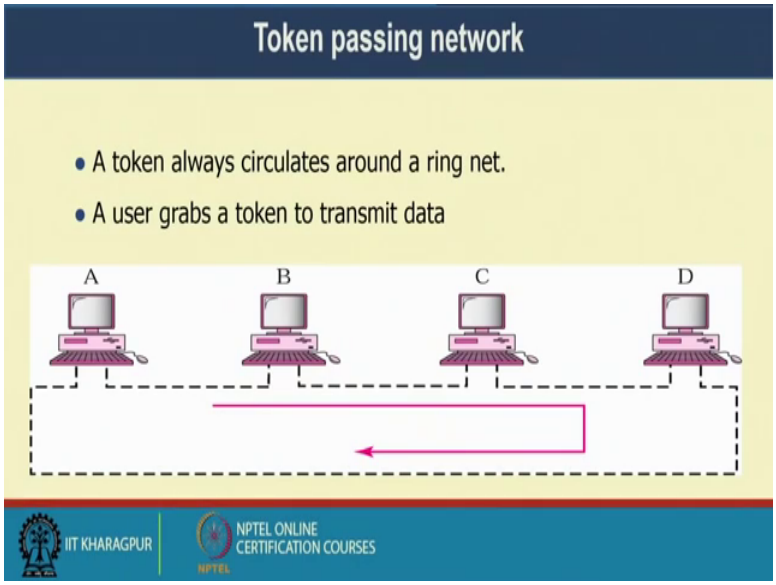


So, control token operation whether ring or bus topology a logical ring is established, right because it has to go on token in the sharing whether it is a physically ring or bus

topology there is a logical ring is established or they token moving or token moving in the ring or token ring type of scenario, right.

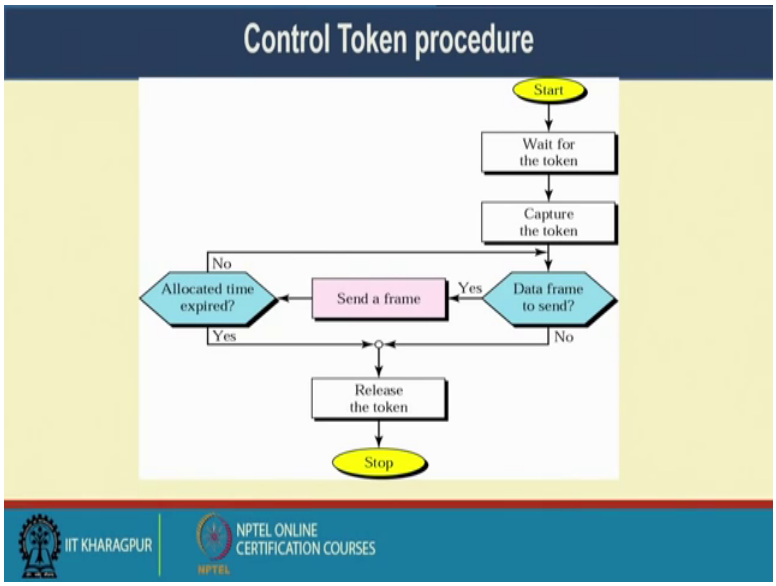
So, logically ring is established which links the nodes using a physical media. So, will see in the next slide that what is the thing. A link control permission token is one node, right the token is passed from node to node around the logical ring until it arrives the node waiting for the center frame so that means, it goes on moving in the node to node unless somebody grabs the token into the to transmit the data. The node captures the token has the control over the token and transmit the data. Upon completing the transmission the node releases the token to the next node in the logical ring. So, in the logical ring it. So, there are nodes which are in the logical ring. So, once that is one ring gets the transmission done it release the token in that logical ring. So, that is the things which you are talking off.

(Refer Slide Time: 23:43)



So, there is a logical ring is has been formed in to the things a token always circulates around a ring net a user grabs a token and transmit the data and this is the logical ring which is formed into the overall scenario, right. So, token is passed from one to another, right. So, the way we discussed.

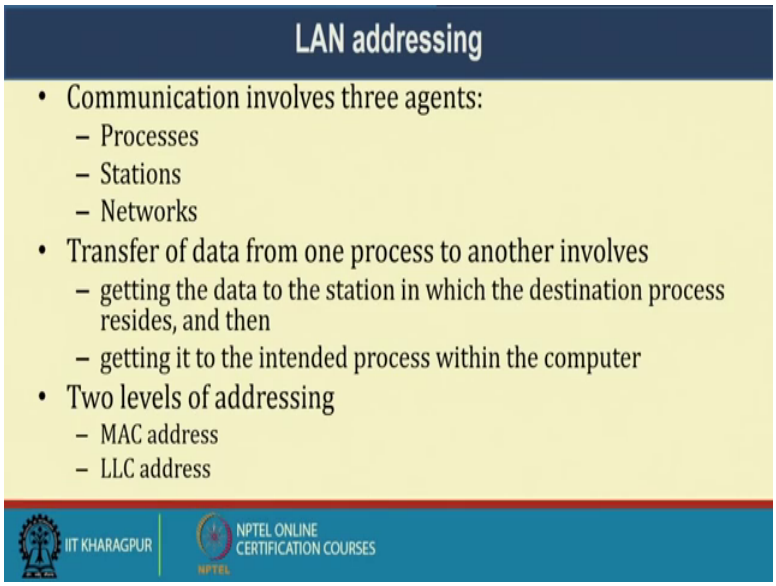
(Refer Slide Time: 24:17)



So, if we try to look at that what we say flow of the thing. So, the wait for the a station need to wait for the token to come, once the token it gets the token it captures or on have the control over the token then it data whether it has a data frame to send. So, it gets the token it so, it has the control over the token if whether it has the it has data frame to send if no then you release the token, right to the next one in the ring or if yes, then send the frame accept the allocated time limit if it is expired then it has to delete the token because it cannot in definitely keep the token on its control its has the there is a time limit for the things. If it is not expired then capture the go to the things again go for the data to be sent etcetera.

In other sense so long it is the token is there till its time has expired it goes on transmitting it goes on transmitting the data it wants to transmit. Once that is once that time is expired then it has to release the thing or its transmission over (Refer Time: 25:42) is not expired it release the token to the next node in the logical ring. So, if these 3 nodes are there if this is the way it is moving. So, it is release to the next node next node next to (Refer Time: 25:53) the logical ring. So, this was in use rather some of the things are still in use, but now it is all mostly over mostly are Ethernet based services or CSMA CD based services what we see these days.

(Refer Slide Time: 26:15)

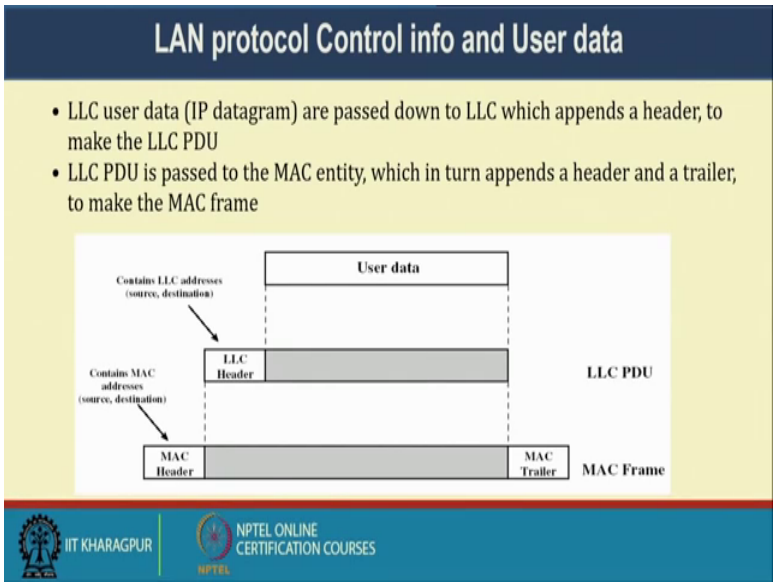


So, there is another important aspect that how this addressing things can come up, right. Communication involves 3 things, right one processes, stations, networks, right. The process to be there their networks is the process used to communicate between the processes and networks the two network, two or more networks are there and the stations which are the in stations.

Transfer of data from one process to another involves getting the data to the station in which the destination process resides and then getting it to the intended process within the computer, right. So, if I want to transmit a data from the things. So, it has to go to that intended process and a execute into the thing.

Two level of addressing they have. So, one is the MAC address or the hardware address or what we sometimes callas network address and there is a LLC addressing scheme where it tries to identify the network service point.

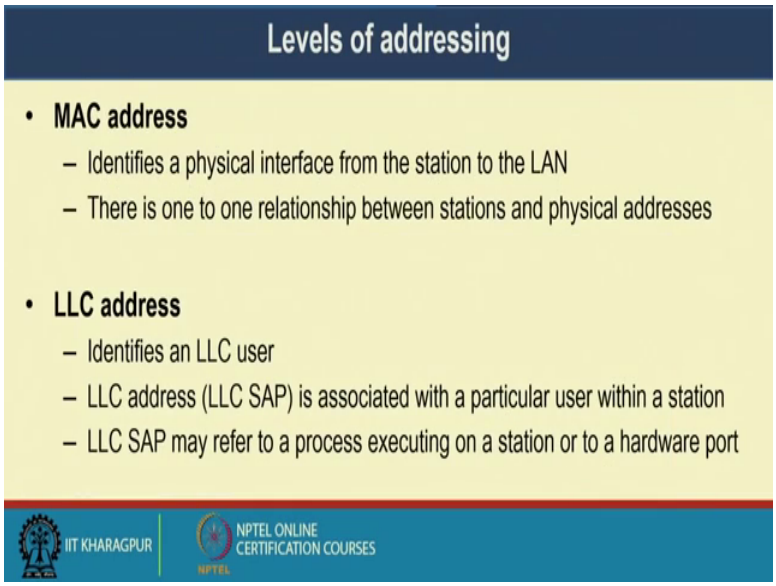
(Refer Slide Time: 27:15)



So, if we look at LLC user data IP datagram are passed now to LLC which appends a header to make the LLC PDU, right. So, with the header it becomes a LLC protocol data unit. The LLC PDU is passed to the MAC entity which in turn appends the header and the trailer to make the MAC frame, right.

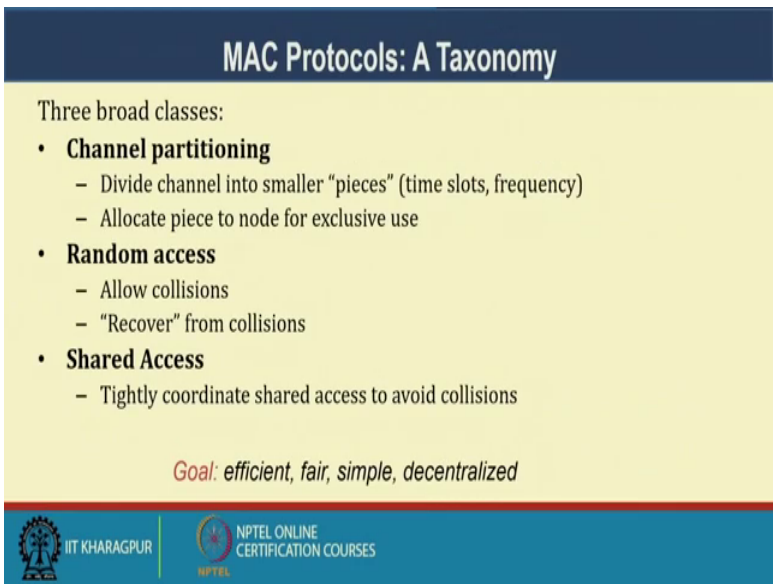
So, I the user data in this case user data in this case what it receive from the upper layer say network layer and then it address the LLC header and create the LLC PDU, this LLC PDU now become the payload for the MAC. So, the MAC adds a header and a trailer and make this MAC frame which need to be transmitted to the next top, right, where the MAC header contains the destination address that is the layer two address of the MAC address which need to be transmitted to the next top.

(Refer Slide Time: 28:19)



So, level of addressing. So, one is MAC addressing identify a physical interface from the station to the LAN, right. So, it should be physically connected wired or wireless there is one or more relationship between the station and the physical address. So, LLC address identify LLC user, LLC address or LSAP is associated with that is a service access point associated a with the particular user within the station, right. And also the LLC service access point may refer to a process executing on a station or to a hardware port end type of things that means, it is mostly talking with the upper layer type of, it is talking with the upper layer type of protocol with the LLC SAP.

(Refer Slide Time: 29:05)



So, what we see; so 3 broad classes or categories, right. In case of if you look at the MAC protocols, so one is channel partitioning like divide channel into smallest piece either time slot or frequency the channel need to be partition, allocate piece to node for exclusive use. So, I allocate these slots into different nodes either through mechanism of CSMACD or token ring and type of thing. So, this is one aspect. Like the channel need to be somewhat logically partitioned and things would be there.

Other aspect is random access allow collisions, allow collision, recover from collision, right. So, one is allowing collision and recovering from the collision. And there is a shared access, tightly co ordinate shared access to avoid collisions, right. So, there is a more coordinated effort to avoid collision, right. So, these are the 3 what we say aspects of MAC layer protocol which is an unto achieve.

The basic philosophy or a basic goal of this thing is that it should be efficient, fair, simple and decentralized, right. So, efficient, fair, efficient means that channel is utilised efficiently; fair means is fair to all the nodes in the in that land like it is not giving any extra preference to the other things, right it should be simple to implement. Finally, end of the day it is these devices are not that high resource devices. So, simple to implement. So, simple and as far as possible it should be decentralised decentralized that there should not be any centralised control over this mechanisms, right. So, that should be decentralized type of things.

So, what we say efficient, simple and decentralized this; these are the things which if any MAC protocol tries to achieve. So, what will what we have seen a overall mechanisms overall basic philosophy of that how this layer two data link layer protocols works. So, LLC and MAC and what are the different technique like CSMACD is the predominant technique which is Ethernet uses also there is a token ring technique things are there and the MAC protocol as such want to become efficient fair to all simple protocol and decentralised.

So, with this let us conclude our discussion today. We will continue our discussion on this layer two or data link layer in our subsequent lectures.

Thank you.