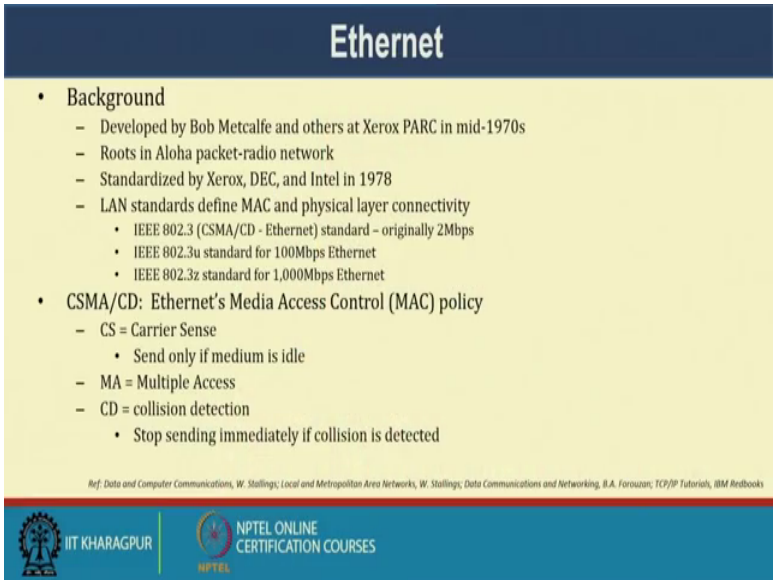
Computer Networks and Internet Protocol
Prof. Soumya Kanti Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 49
Data Link Layer-Ethernet

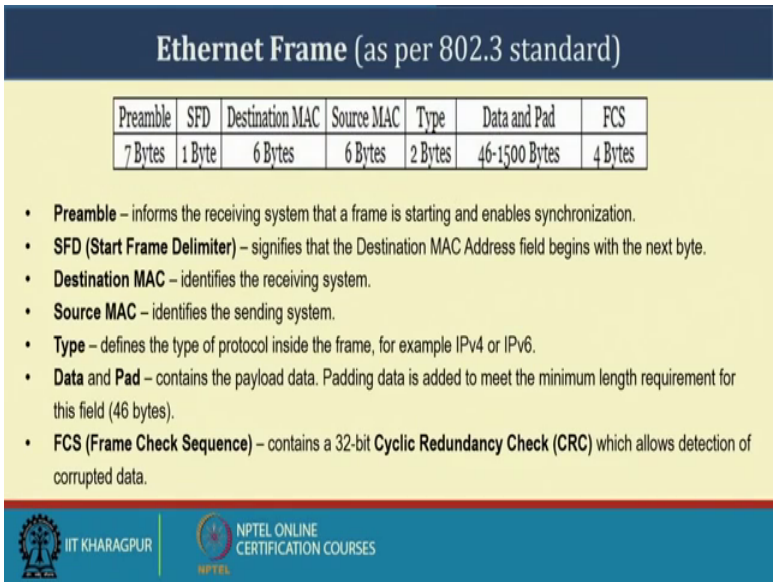
Hello. So we will be continuing our discussion on Ethernet. What we are discussing in the last lecture on Data Link Layer phenomena under this Computer Networks and Internet Protocol course right. So, as Ethernet is one of the predominant technology in the layer two devices and omnipresent across the network. So, we already discuss some of the aspects we will be trying to cover some more aspects here. So, it gives as a overall idea that how the Ethernet works right.

(Refer Slide Time: 00:55)



So, just to a recap slide it was developed by Bob Metcalfe in Xerox PARC an (Refer Time: 01:02) in 1970. So, basic motivation from the Aloha packet-radio network standardized by Xerox DEC in 78. And there are few standards which became pretty popular 802.3 which use's CSMA CD. 802.3 u for 100 Mbps standard Ethernet and 803.z 802.3 z which is for gigabit Ethernet or 1,000 Mbps gigabit Ethernet and it implies CSMA CD.

(Refer Slide Time: 01:42)



So, just to give a Ethernet frame last lecture also we discussed, but there are little bit maybe some ambiguity, but to clear it off the Ethernet frame is as far as 802.3 standard constitutes a preamble. If you remember one some slide some of the literature means in preamble consisting of a 7 plus 8 bit. But as per the standard preamble is a 7 byte; sorry, it by 7 byte, SDF is 1 byte, destination MAC is 6 byte, source MAC is 6 byte, type is 2 bytes, payload MAC's is 1,500 bytes, 46 to 1,500 bytes. So, if the there is no payload I we should have at least a padding of 46 right. So, if I say the payload where is from 0 to 1,500 bytes, the pad where is from 0 to 46 bytes and we have a CRC check or FCS of 4 byte right. So, preambles inform the receiving system that a frame is starting and enable synchronization right.

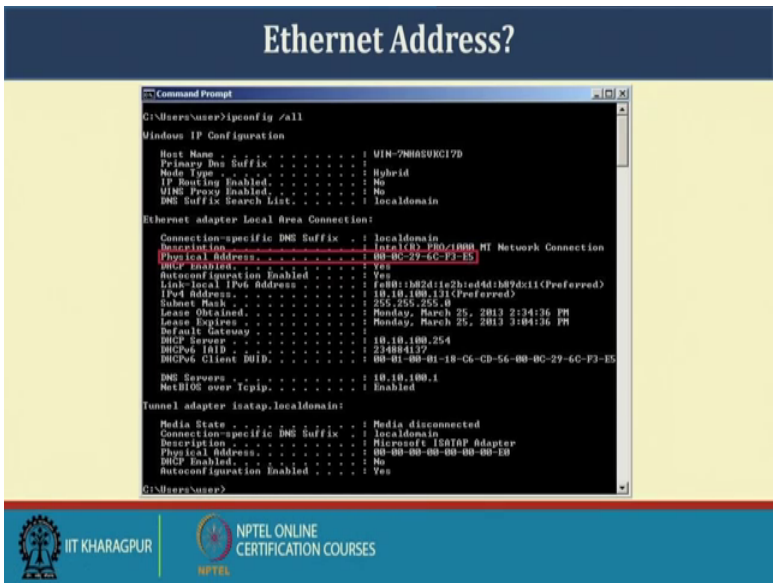
So, that start of that it say it for the synchronisation it says the receiving systems or inform the receiving system the frame is starting. SDF or the start frame delimiter is signifies the destination MAC address field begins at the next byte. So, it says that the next byte onwards the destination MAC address is there or that the hardware address on network address, online address whatever we say.

So, destination MAC address identifies the receiving system, source MAC address identifies in the sending system, type identifies the protocol inside the frame. That means the next higher level protocol. Typically for example, it maybe IPv4 and IPv6 right and data and pad contains the payload data right. What is received from the higher level

protocol? The payload data and padding data is added to meet the minimum length required for the field. So, the minimum length required for this field is 46 byte. So, the padding is added for that if the pad there is no payload; that means, 0 thing is if theoretically. Then the padding of 46 will be there if the full payload 1,500 bytes are there then I may it may not have any padding right. And the frame check sequence typically the CRC contains a 32 bit, CRC redundancy check which allows the detection of the corrupted; so that is the frame check sequence or FCS. So, this constitutes the typical Ethernet frame a preamble 7 byte, SDF 1 byte, destination MAC address 6 bytes, source MAC address 6 byte, type 2 bytes, payload 46 to 1,500 bytes and payload plus padding so it should be at least 46 bytes and FCS of this right.

So, if we keep away this preamble and SDF so we required 14 bytes at the beginning and 4 byte at the end. And these are primarily two more of synchronisation and say that were the start of next address is there and like sort of this right.

(Refer Slide Time: 05:20)

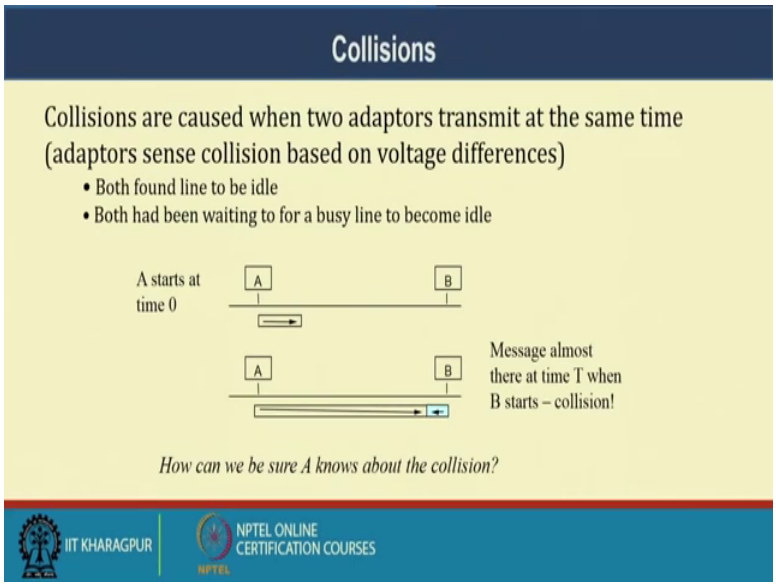


Now how do I know the MAC address; many of you might I tried. In Linux there is a command call IP Config if you give slash all then it keeps on MAC address of the thing right. In windows there is there is IP Config in windows it is IF config let just try if it works right. Now if you let me see whether I can expand it will let us see you can use the command called IF Config. And you see here the MAC is MAC address is all if you see IP Config minus slash all so where is the MAC here is the physical address right 64 00

6a ic 1 is 63 right. So, this is the typical MAC of this particular systems where from where this we I am using the systems right. So, it is in case of this is I if this is IP Config slash all here also we have used this ok. It is in windows only in the in case of Linux it is IF Config right; anyway that commands you can get easily.

So, in other says what you want to say that you can basically get in good get around this MAC address or the physical address of the things. And we see that is the 48 bit structure 18 to 6 we signifies the MAC address of the particular systems. So, when we communicate we require the source and the destination and as let me repeat it, but when every hub that MAC need to be resolved right. So, when I hub from one system or one router or any network device to network device every link the hub the magnate it to reserve for the destination and it is transmitted to the destination right.

(Refer Slide Time: 07:43)

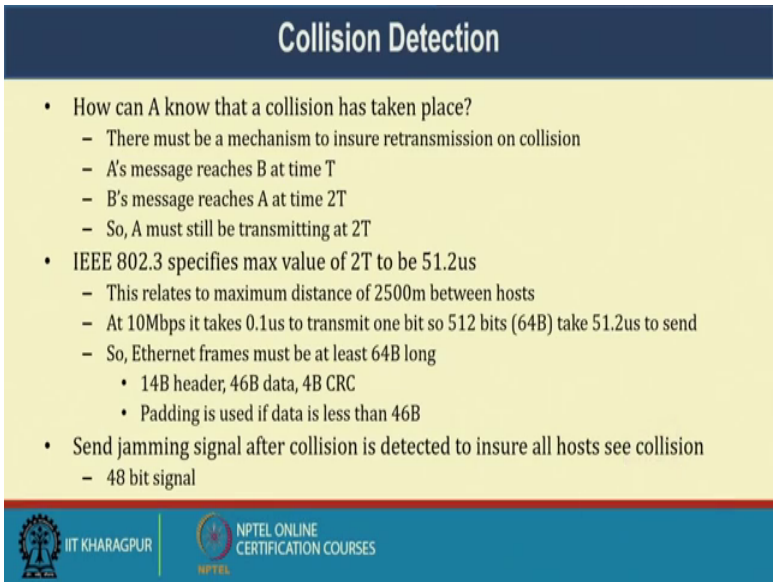


So, the major challenge when we have a said media is collisions right that. So that is why carrier sense multiple access with collision detection scheme right when you say for a wired media. We later on will look at in sometime we will look at the other mechanism for wireless media; where we have a instead of a collision detection a collision avoidance scheme. Because there are detecting collision in a wireless media is much difficult in that will come to that sometime later in this particular course. So, collisions are caused when two adaptors transmit the same time adaptor sense collision based on the voltage differences right. So, the how the collision is caused when the two adaptors without

knowing that both are thinking or both are sensing channel to be free and communicate and then it is collide.

And there is a once the collision is there is a fluctuation in the voltage the adaptor understand the voltage like A is sending to B. So, at time 0 it start where as more only set the same time or after a typical delta T time the B starts where, also it sense this so somewhere here the it collides in between collides. And then the voltage fluctuations difference among the things unless A gets a sense of that voltage difference is it thing it is gets A and B both things that there is a collision. It sense a jam packet and resend the retransmit after the sometime right.

(Refer Slide Time: 09:28)



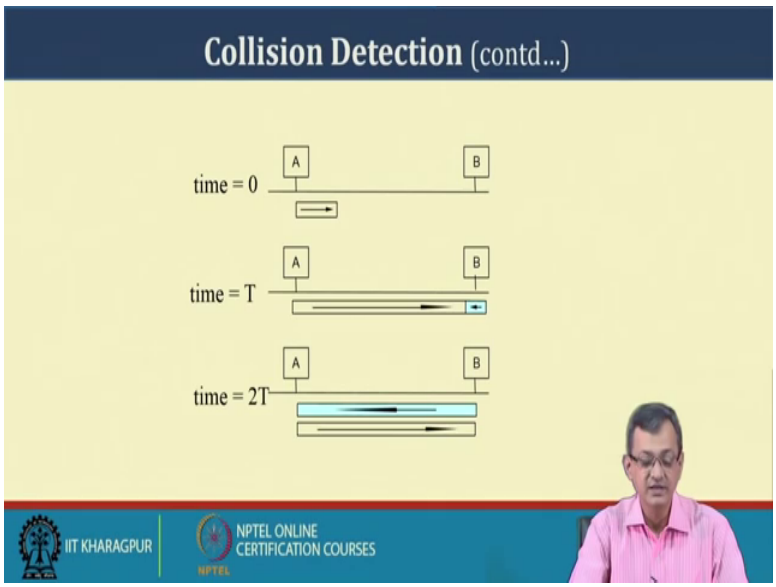
So, how can A know that a collision happens? there must be a mechanism to insure transmission retransmission on collision right. Otherwise we do not know that where the data it at send and then there is no data where I think so there otherwise retransmission is there. If that is not there so it is typically some sort of a connection or best effort service you transmit and then forget that whatever as gone one right. So, A is message reaches B reaches B at time T so B is message from the B to A it is 2 T. So, a must still be transmitting at 2 T; so after 2 T time it may know that there is collision or not.

So, 802.3 specifies max value of 2 T to be 51.2 micro second ok. Last class also we have seen this relates to a maximum distance of 2,500 meter between the host which at 10 Mbps speed in 0.1 micro second 1 to transmit 1 bit to. So, 512 bits takes 51.2 micro

second. So, it takes point in 10 Mbps to transmit 1 bit it take 0.1 micro second for in 51.2 micro second. It will be some 512 bits or] 64 bytes of data to transit. So, the Ethernet frame must be 64 byte long so that you can it can faithfully recognise or identify a collision. So, out of that 14 goes on the header excluding that first 8 byte of preamble and SFD and the 4 byte goes for the FCS or the CRC check. So, 46 byte of the payload is minimum required otherwise I cannot guaranty that whether I can find out the things.

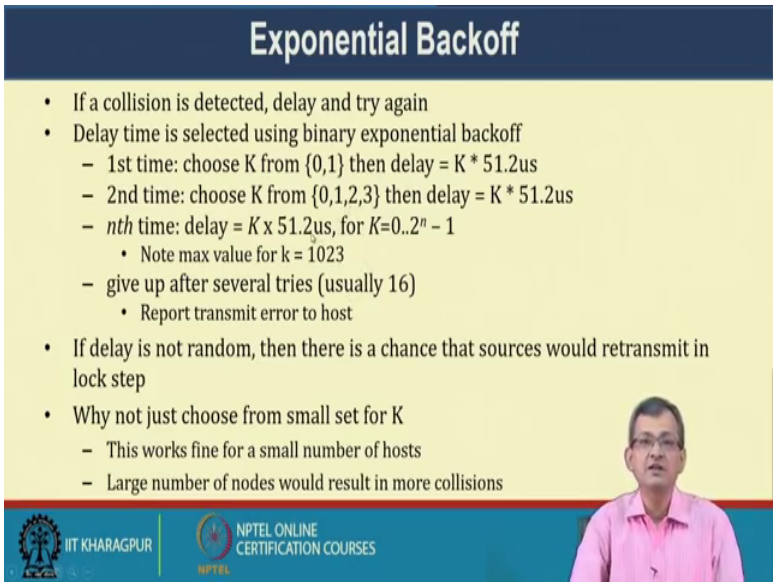
So, that is why what we see that the payload length has been specified, specified from not 0 to 1,500, 46 to 1,500 bytes right. So, or the in other sense 0 to 1,500 is the padding or 0 to 46 is the or in a sense 46 to 0 is the hey sorry data 0 to 1,500 is the data 0 to 46 or 46 to 0 is the padding of the data. So, that is the requirement of the of that particular payload field. So, if there is a collision it sends a jam signal after collision to detect to insure that all host know all host know about the collision or see the collision. So, it is a bit 48 bit signalling mechanisms.

(Refer Slide Time: 12:30)



So, there is a same picture, there is a collision, and there is a retransmit this there is after 2 T time a gets that informational collision and then it goes on retransmission.

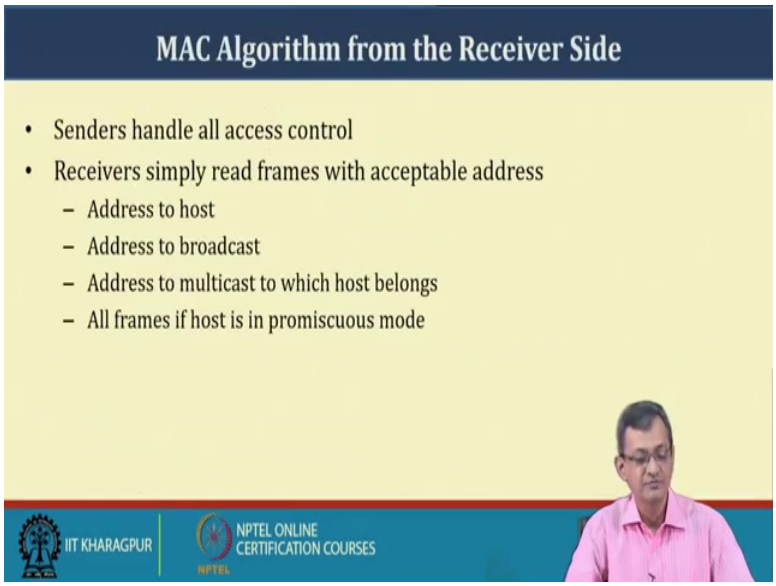
(Refer Slide Time: 12:41)



So, if a collision is detected delay and try again; that is the philosophy it is not that immediately retransmit delay, sense, try again right or try again in the sense again sends the channel and then plumb that in. So, first time choose K how much time you will there K from 0 one then delay for K into 51.2.

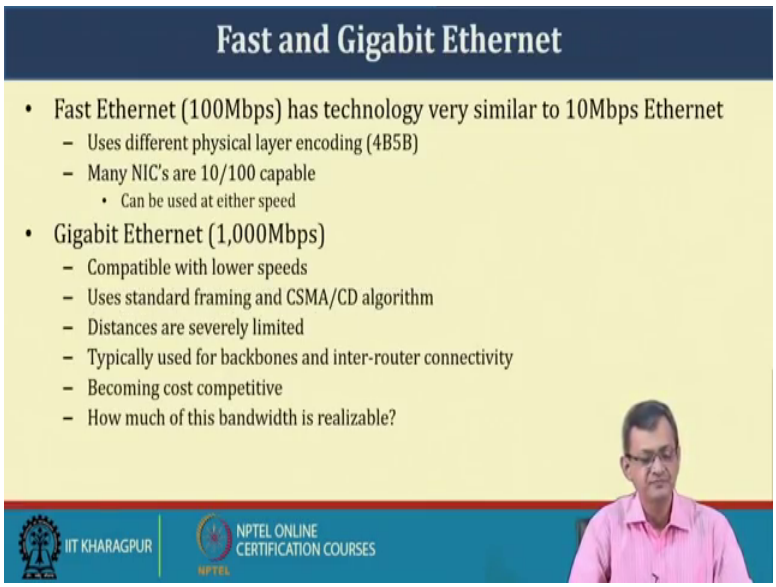
So, second time choose K from 0 1 2 3; nth time K 0 to 2 to the power n minus 1. The maximum value of K will be 1023 this we have seen also right. If the delay is not random there is a chance that the source would retransmit in lock step. And if it is a very small then it is fine for small network, but it may be problematic or large number of nodes will result in more collisions in a (Refer Time: 13:36).

(Refer Slide Time: 12:36)



So, from the receiver side send a handles all access control right from the receiver is simply read the frames and acceptable address. So, address to host, address to broadcast, address to multicast, to which the host belongs all frames if the host is in the promiscuous state right; so this is the receiver things right if it wants to do with the receiver it.

(Refer Slide Time: 14:10)

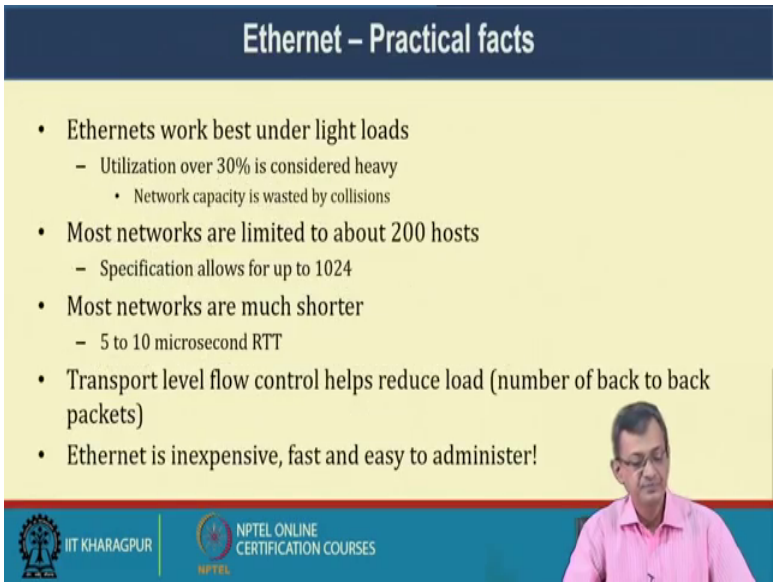


So, there is a another; so what we are seen sometimes will down the today's talk itself will see that gradually how it evolved just to recap the things that how it evolved putting

all this together. So, with the increase of requirement of bandwidth and more bandwidth hungry applications at said that so we the overall graduate it from fast Ethernet and gigabit Ethernet. So, fast Ethernet which gives a 100 Mbps has technology very similar to 10 Mbps uses different physical layer encoding 4B 5B will see that when we will discuss about the physical layer sometime in this lecture series. And can be many NIC's has both 10 slash 100 compatibility.

So; that means, it switches based on the things it negotiate and find out that were things will be there. So, other thing is the 100 Gbps or gigabit 100 Mbps of the gigabit Ethernet compatible with lower speed uses standard framing and CSMA CD algorithms distance are severally limited typically used in the backbone and inter router connectivity. So, it is a high speed things where the backbone and inter router connectivity become becoming cost competitive that become the cost is slowly coming down and it is becoming more viable. And that finally, it need to be seen that how much effective bandwidth is real able realizable that is also need to be calculated on need to be evaluated type of things.

(Refer Slide Time: 15:55)

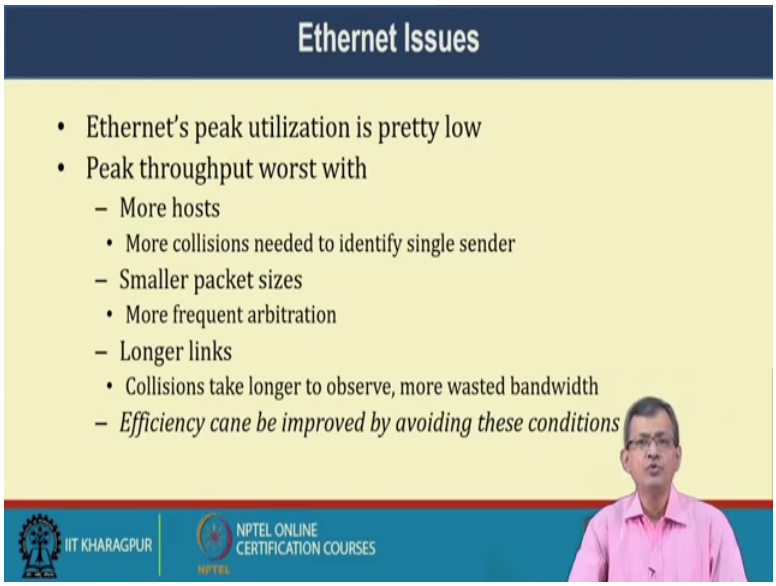


So, if you look at the Ethernet; Ethernet works best under light loads utilization over 30 percent is considered sometimes heavy nodes load. Network capacity is wasted by collision what I am telling that traditional Ethernet. Most network are limited to about 200 nodes to specification allows up to 102 for nodes, but mostly when we say that within a particular network then we have a 200 nodes. Then we will see the concept of

bridged a land that we have a bridge to connect the other land. Most networks are much shorter 10 to 5 to 10microsecond that RTT.

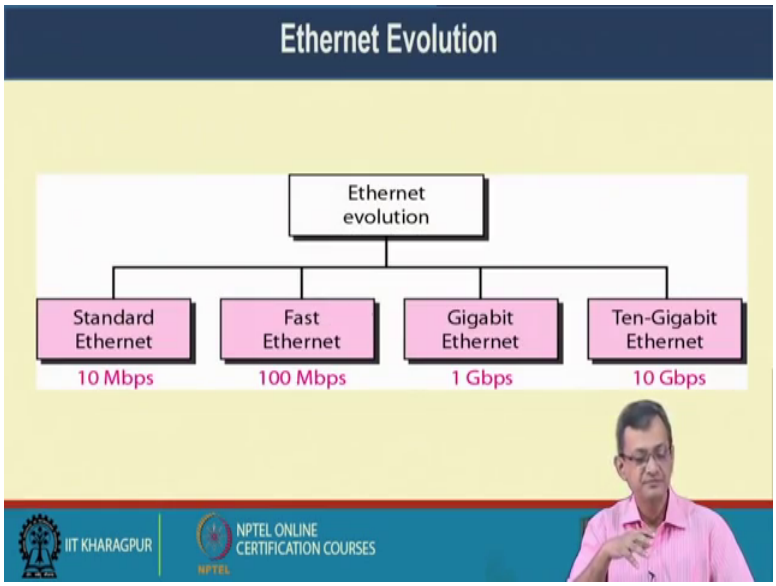
And now (Refer Time: 16:40) transport level flow control helps reduce load. So, as we are talking about that there are the other layers what they are doing it is totally not keeping independently the transport layer flow control mechanism may help in reducing the load Ethernet is inexpensive so to say fast and easy to administer right. So, Ethernet found to be cost effective quite fast and easy to administer overall. So, it is a from the network administration station point of view it is always a good thing to do to look at the things.

(Refer Slide Time: 17:20)



There are a few challenges issues or with this Ethernet I am that some of them ask Ethernet peak utilization is pretty low right. So, it is low peak throughput worst with more hosts. So, if you connect more hosts that the throughput will fall more collision needs to identify by a single sender smaller packet size more frequent arbitration. Longer links collision take longer to observe more wasted of bandwidth if it is a link is longer than it is a more collision takes in a large time to works we have seen that 2 into T efficiency sorry there is a typo can be improved by avoiding this condition.

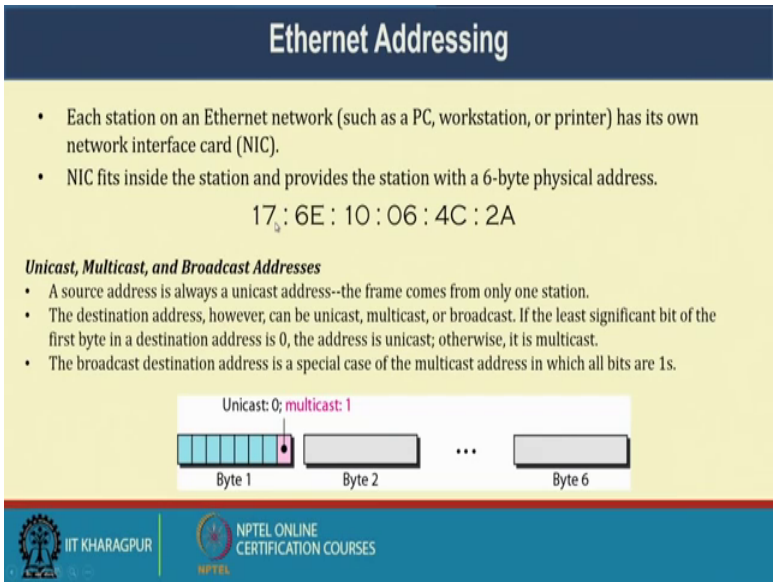
(Refer Slide Time: 18:19)



So, see these are these are may be admistadibly control and later on we will see that there are things which we can which can be managed we can manage with this Ethernet. So, this can be improved by avoiding these conditions. So, if we come to this overall evaluation of the Standard Ethernet. So, we have Standard Ethernet, Fast Ethernet, Gigabit Ethernet, Ten-Gigabit Ethernet. Now a days we are talking about Ten-Gigabit Ethernet we see that there is a issue of bundling this things to larger bandwidth and so and so forth.

Mostly use for higher things are mostly used for backbone traffic because in because neither the application nor the most of the devices can exploit that that very high level. Because I have a laptop with some 100Mbps capability connecting to a 1 gigabit so it is wastage of the resources right. And secondly, all are not used even your connectivity is at 1 Gigabit or 100Mbps. Finally, your application may not be using more than 10Mbps or 20Mbps and type of things like that so it is a again a wastage of resources. And whenever you go up on the scale on the speed the cost increases manageability becomes challenging and it is a overall pressure on the backbone of the network.

(Refer Slide Time: 19:33)



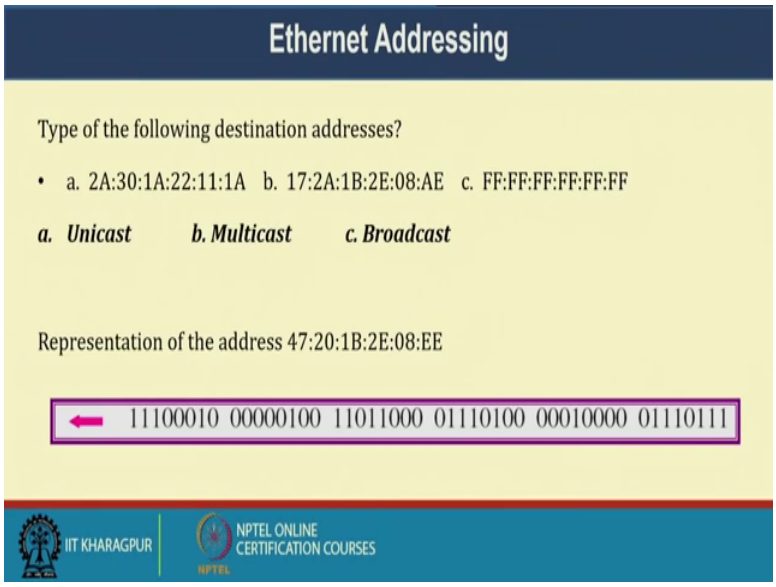
So, Ethernet addressing already we have seen just to recall. So every each station on a Ethernet network or every system on an Ethernet network such as PC, workstation, printer etcetera. Which on network enabled having a network interface card has it is own network interface card or NIC right. So, in these systems like this system's out I am using here. And it is a own NIC your network interface card has adapted to connect to the physical media, it can be wired connection, it can be wireless connection, it can be coaxial cable, it can be twisted pair, it can be fibre optic, it can be some wireless devices Bluetooth, etcetera. NIC fits inside the station and provides the station with a 6 byte physical address which is unique for every NIC ideally.

So, typically like 17 6E 10 this is a typical thinks 6 byte address right and there is a scheme at the layer two level is a Unicast multicast and broadcast address right. So, a source address is always Unicast right so fine it is generating it is always Unicast the frame comes from only one station. So, anyway generating a Ethernet or layer two frame it comes from a one station the destination address.

However, it can be Unicast multicast or broadcast if the least significant bit of the byte in the destination is 0 the address is Unicast right or otherwise it is multicast right. So, say this address what is this 7; 7 signifies 0 1 1 1 so; that means, the least significant bit of the; a as you have seen the that is similarly of the first byte in the destination address is not 0 in this case 1 so that means, it say multicast. Broadcast address is a special case of

multicast in which all bits are 1 what does it mean that all these are ones in other sense this is a FF:FF:FF:FF:FF:FF right: 6 FF right. So, that is the multi there is a broadcast a special case of a multicast.

(Refer Slide Time: 21:56)



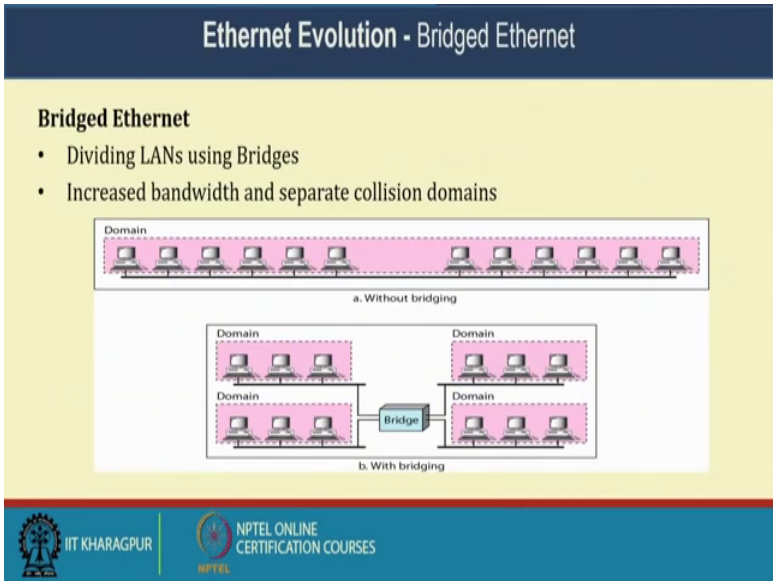
Like here, if we have this A as the BC so a is a Unicast because a is 0110 right. Any way last bit is 0 for this first this one these the last bit of the first byte is 1. So, it is multicast and these are all one"s so that is broadcast right. And if I have a address like this there is maybe there is some typo because this is not representing directly here because this 47 it is not representing 47. So, just please re calculate this one it should be some a typo is there any way. So, what to be mean to say when we took at address like this it is decipher into the binary form right.

So, again I am repeating this 40 yes please check the representation. This 47 should be representing here, 20 representing here, 1B representing here, 2 here at the 47 is not this representation right. Because 4 is 0 0100 0100 and 7 is 0 111 so it is should have been 01000111 so there is a mistake here there please correct it.

Anyway these are the bit wise representation and when it goes it goes in this direction. So, the when did you send that is going and receiver receiving it is in this direction. Now if you look at the standard Ethernet already we have discussed. So, it is 10 base 5 bus thick coaxial 10 base 2 it is say again bus structure with thin coaxial 10 base T is the

twisted pair that is which allows star connects start type of topology 10 base F is a fibre with star topology where 10 represent the speed of the thing.

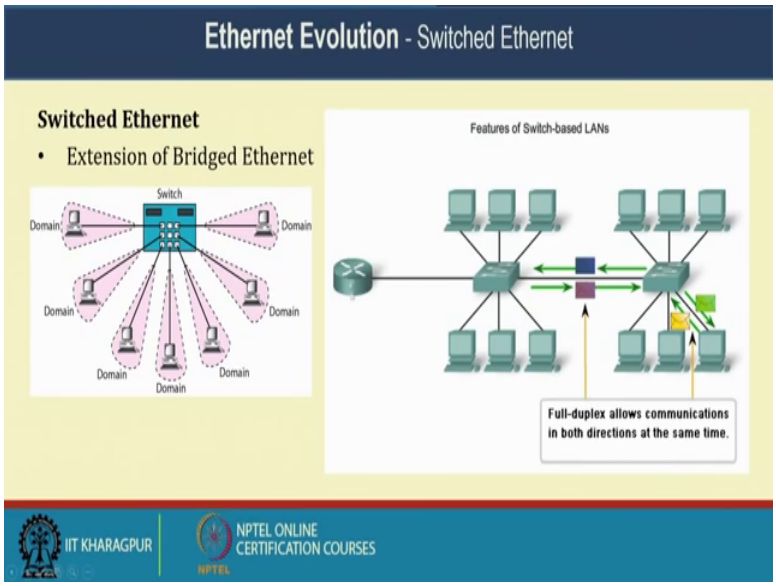
(Refer Slide Time: 24:04)



Ethernet evaluation bridge Ethernet dividing LAN's using bridges increase bandwidth and separates collision domains correct. So, if I have a large number of systems into the things so there is a concept of bridge Ethernet right. So, I we put a bridge in between so what happen that instead of this one whole thing I put we can put a bridge here. So, these two LAN's are now connected with a layer two device or bridge. What it does it basically as we know layer two device divides a collision domain the collisions are they are separate collision domains and in a effect it increase the overall bandwidth.

So, this is the bridge Ethernet where we have better bandwidth things. So, if you look at your own network in your office; or in your colleges, offices and so where the number of networks are there. So, at least we have layer two devices which are which basically a divide the collision domain effectively increase the bandwidth of the network right effective bandwidth of the network is increase or in other sense the wastage of the bandwidth due to collision are reduced. So, that is a very standard practice to do that so divide LAN's into bridges.

(Refer Slide Time: 25:34)



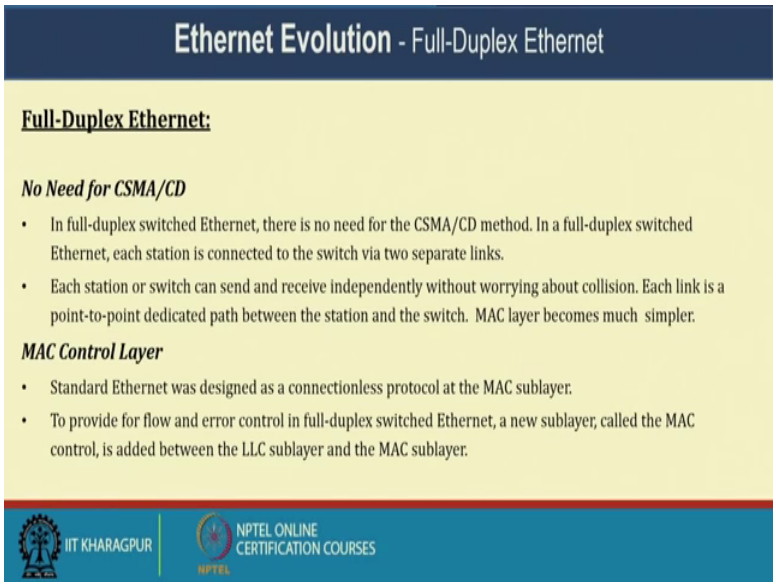
So, we have the next phase the bridge to switch can be thought of what we can say a multiport bridge. So, instead of one bridge dividing into two; I can have now a switch of 12 ports which is dividing into 12 domains right. So, as per domain which again can connect to the bridge so, I can have a hierarchical structure of this layer two devices right which allows me to increase the effective better utilisation of the bandwidth of the available network right. Like here we have one set of switches which goes on things another a switch which connect a set of systems say this is a router or layer three device right.

So, it is a in this connection it is a full duplex connection it come to that so trans received is difference. So, there is a not a challenge of collision, but a effectively we can manage the things and as you know that these are there are manage switches and type of thing. So, we can basically understand manage the switch in effective manner that how the switches can be managed and type of things in effective more effective manner. So, there we have the overall health of the switch or management of the wave switch.

Next one is a full duplex Ethernet which is popular these days which are switch are mostly used these days in most of the today's network. So, full duplex network mode increases the capacity of the each domain to 10Mbps to 20mbps. So, this is full duplex as we are showing the pixel that is full duplex. So, or it increases in a doub in somewhat double in other sense we have a separate transrecieve line. So, they are not colliding each

other in the transmitter and the receiver or not colliding with one another. So, that that increases effectively so something 10Mbps effectively increased to 20Mbps. So, all are transrecieve lines are different.

(Refer Slide Time: 27:46)



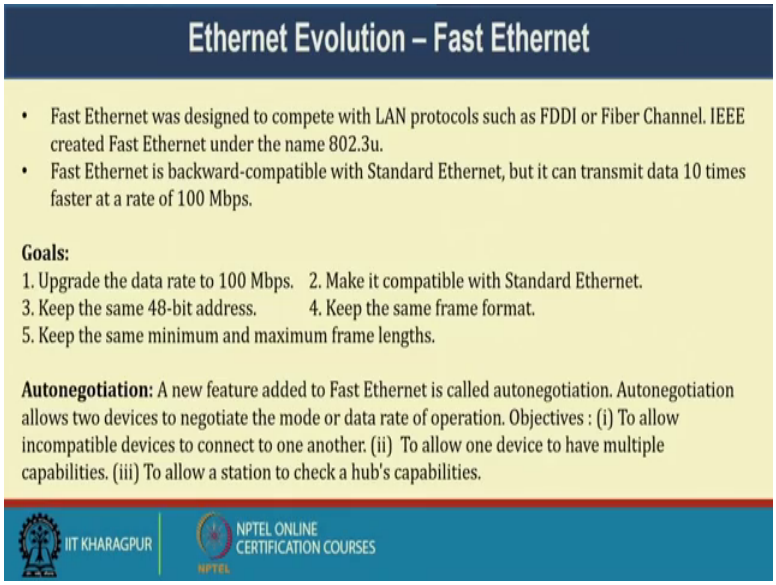
So, in other sense what we say in a full duplex Ethernet that may not be need of any CSMA CD because there is in a separate transreceive. So, there is a no collision parts say right in a full duplex switch Ethernet there is no need of CSMA CD method in a full duplex switched Ethernet is station is connected to the switch via to separate links right. So, we have a transline and a receive line so each station or switch can send or receive independently without worrying about the collision each link is a point to point dedicated path between the station and the switch. And the MAC layer becomes much simplier in this case, because into do not have to take care all those things of the collision avoid a collision detection and type of things are.

So, in other sense what we are saying these days whenever this system is connected to a switch it is as a two's trans two separate line one for trans and another for receives right. So, in other sense it has it has independently that transrecieve things goes on there is no collision so there is no need of CSMA CD part say. So, there is a MAC control layer standard Ethernet was designed as a connectionless protocol for MAC sub layer right. So, if you look at the standard Ethernet it was more of a connectionless protocol like you transmit and you do not manage the thing to provide for an error control in a full duplex

Ethernet a new sub layer call MAC control is added between the LLC sub layer and MAC layer sub layer.

Now we need to have something what we say flow and error control mechanism within the Ethernet right. So, if there is a error of transmission; that means, you send the packet the packet is not reached you have sending an acknowledgement it is dropped. So, there is both. So, that hamper that error control error hampers overall slow mechanism of the things because ethernet what we see layer two is a hub by hub, but end of the day it has need to transmit across the thing. And in most in several cases in it requires some sort of a flow control error control mechanism to ensure a some sort of typical service level assurance or quality of services and type of things.

(Refer Slide Time: 30:05)



So, first Ethernet already we have a seen so was designed to compete with the LAN protocol, FDDI, or fibre channel IEEE created fast Ethernet 802.3u has a rate of 100 Mbps. So, goal upgrade the data rate to 100 Mbps make it compatible with standard Ethernet keep same 48 byte addressing scheme keep the same frame format. So, there is no incompatibility keep the same minimum and maximum frame length so those are kept.

So, there is a there is a feature added to fast Ethernet in is a auto negotiation. New feature added to fast Ethernet is call auto negotiation. Auto negotiation allows two device to negotiate the mode or data rate of operation right. So, which mode and which data rate

operations to allow compatible devices to connect to incompatible devices to connect to each other that will allow one device to have multiple capabilities right. So, it can connect to 10 Mbps 10 slash 100 this type of things are possible to allow a station to check the hubs capability like it if is a managing then I can check that how much capabilities there. And accordingly, I the station can transmit so hub or switch we can this is loosely used so it is so allow the station to check the switch capability.

And finally, the what we are the next evaluation on the thing is the gigabit Ethernet higher data rate of 1Gbps in full duplex mode gigabit Ethernet there is no collision the maximum length of the capable a cable is determined by the signal attenuation in the cable. So, that is the only things which is there and there are different various in of the things and these days we are having ten gig Ethernet and so and so forth. So, these are some of the evolution of the things.

So, what we do with this we let us conclude today's lecture on a overview or the overall that basic functionality or Basic Concept of Ethernet. So now, will in the subsequent lecture will look at more aspects of layer two or data link layer of this, but overall a overall network a layering or the OSI or TCPIP layer.

Thank you.