Real-Time Systems

Prof. Dr. Rajib Mall

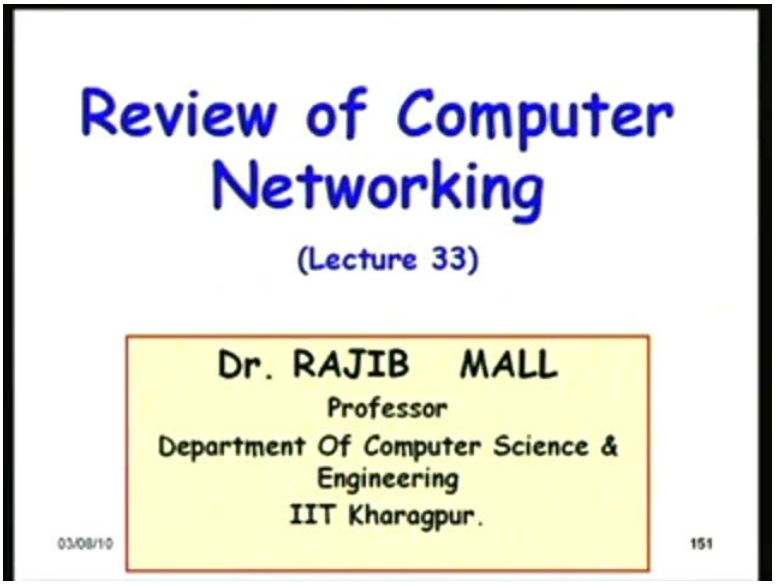
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Module No. # 01
Lecture No. # 33

Review of Computer Networking

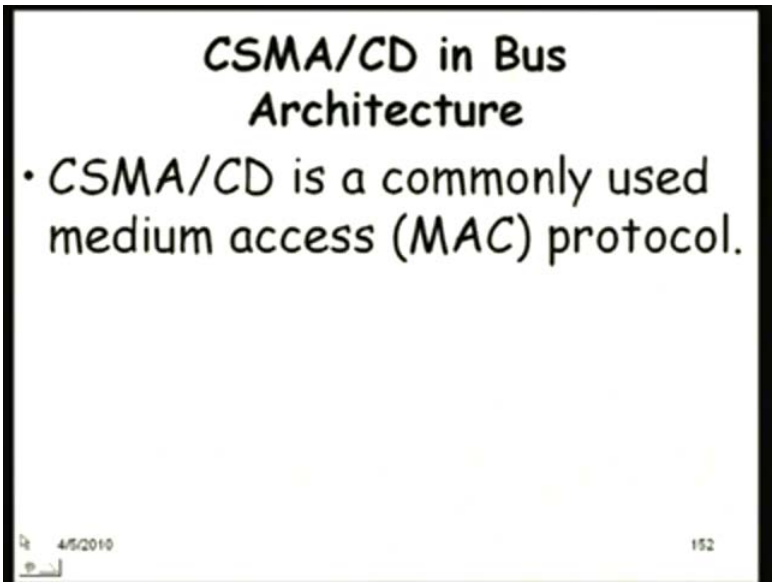
So, let us proceed from where we left last time. We were discussing some basic issues in real time communication. But before we proceed further on the real time communication, I thought, may be a good idea to review some basics issues in computer networking so that those who already know this will refresh their knowledge, and those who did not know much about computer networking, they can be on a footing where they can cope up with the discussions that we have in the subsequent hours.

(Refer Slide Time: 00:58)

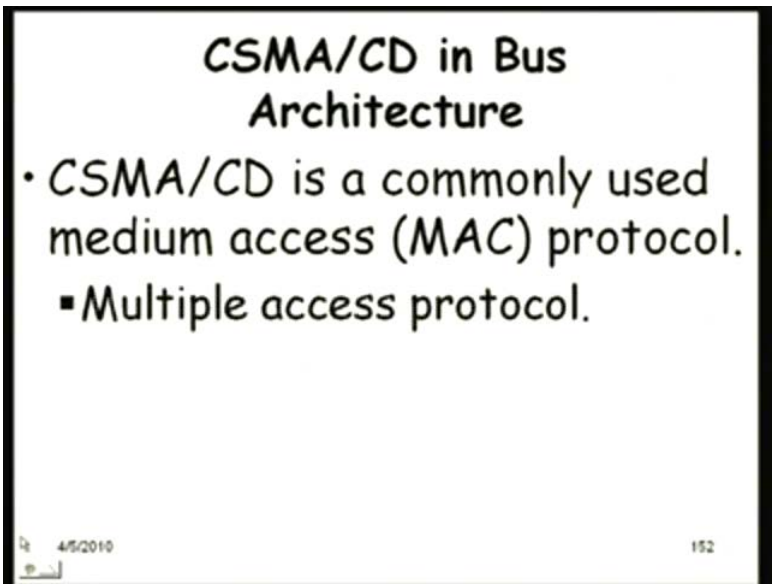


So, let us proceed from there. We will spend an hour to review some computer networking issues which will appear again and again in our discussions later on.

(Refer Slide Time: 01:12)

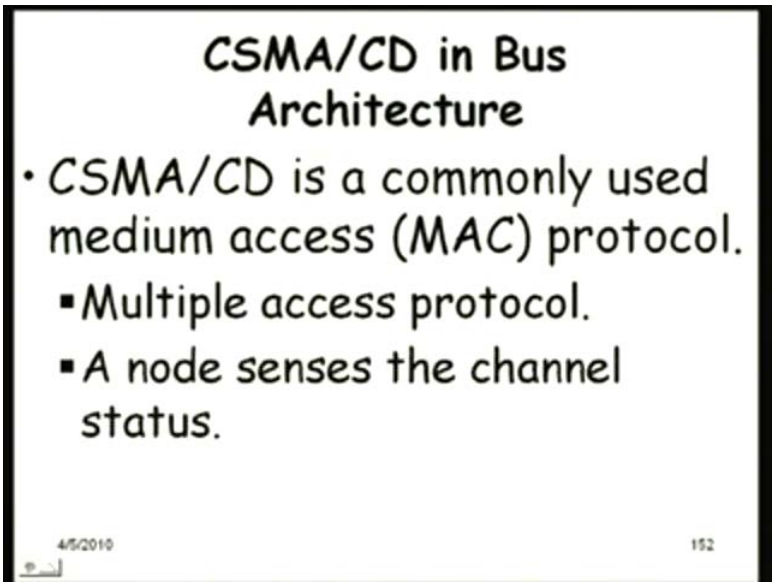


(Refer Slide Time: 01:14)

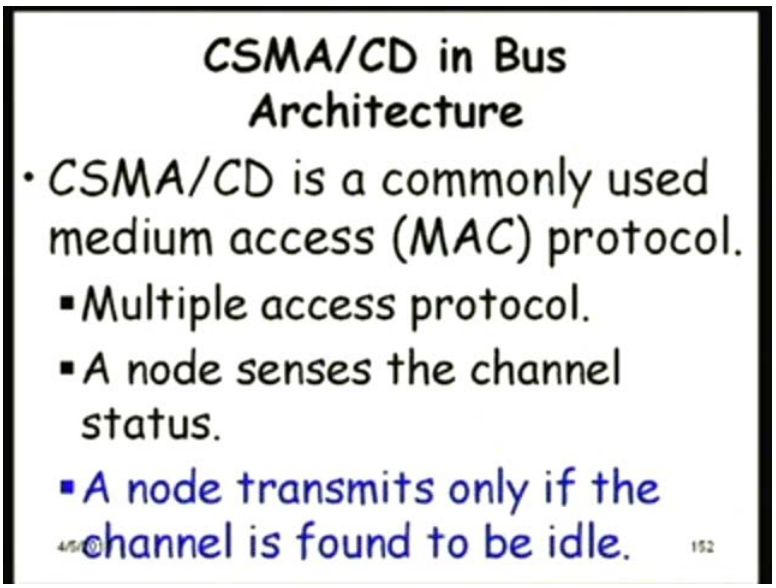


So, CSMA/CD is a multiple access protocol. We will not spend time because requirement for this course was basic course on computer networking. So, this is the medium access protocol.

(Refer Slide Time: 01:27)

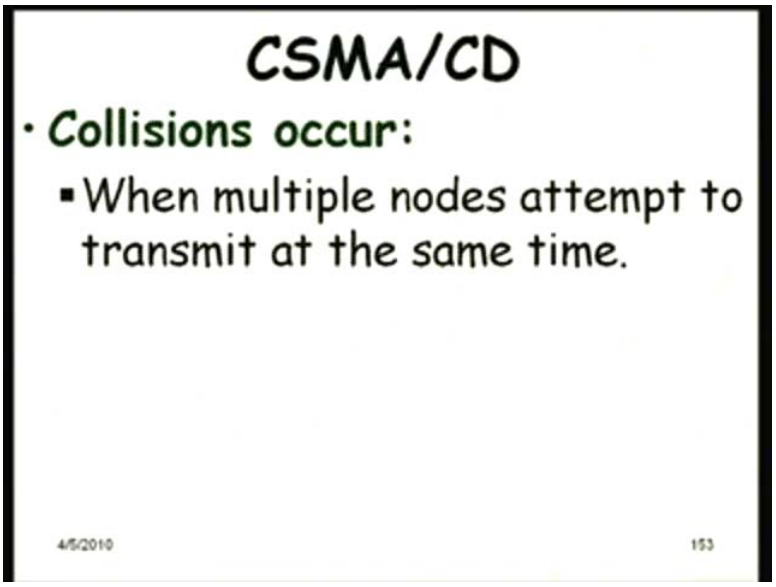


(Refer Slide Time: 01:29)



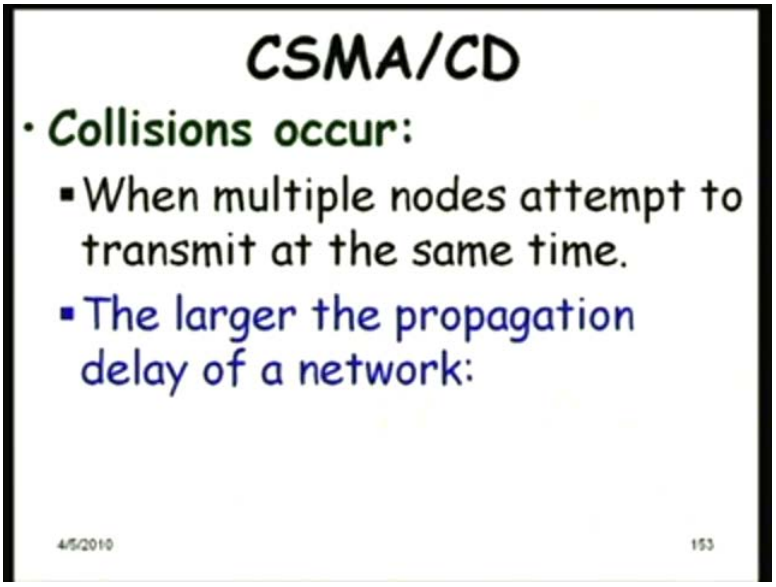
Node senses the channel status and if the channel is found to be idle, then the transmission begins.

(Refer Slide Time: 01:37)

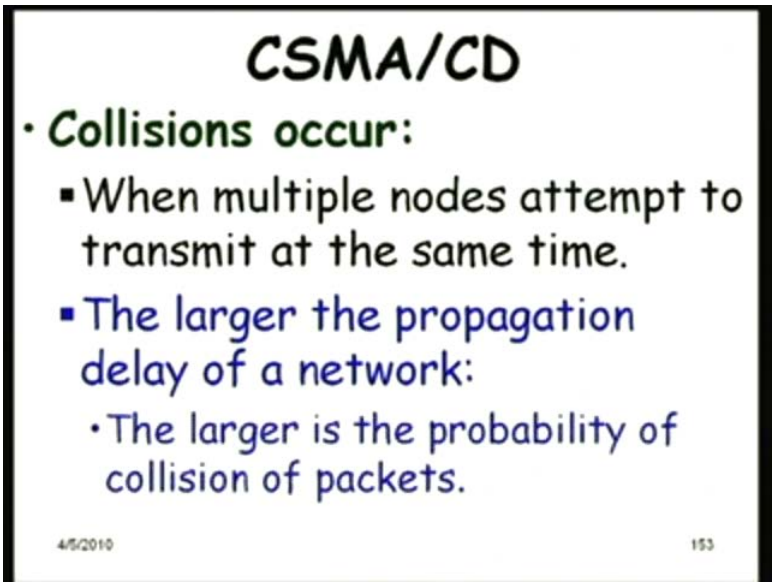


When multiple nodes attempt to transmit at the same time, collisions occur.

(Refer Slide Time: 01:42)



(Refer Slide Time: 01: 51)



But one thing that, we must understand is that the larger the propagation delay of a network, the larger is the probability of collision of packets. Do you agree with this? So, why is that?

((They are)) holding the channel for longer time.

What do you mean by holding the channel? See what we are saying is larger is the propagation delay, we had discussed about propagation delay; the time the signal the time it takes for a signal to propagate or travel from one end to the other end or from the point where the node is attached to both the ends, the time it takes.

(( )). No sorry.

(( ))

Can you please repeat again?

(( )) large propagation.

Large propagation yes. The same transmission time for other station. Yes

(( ))

Let us see if somebody else is telling anything. So, what is your opinion? Why is it that the larger is the propagation time, the more is the chances of collision.

(( )) Yes.

(( )) is in between the other station (( )) probability that another station (( )) transmits is more.

Not clear. It is not that complicated. See the answer is that, see a station transmits after sensing the channel to be idle. So, it may so happen that it has sensed the channel to be idle, but by that time, some other station had already started transmitting, and it is taking time for it to reach here.

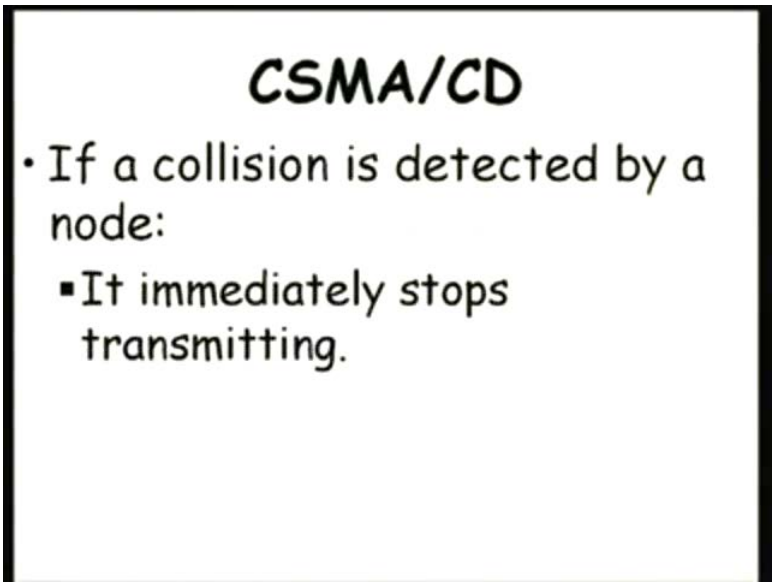
So, the more is the propagation distance, the more is that difference where the other stations could initiate the communication, but other channel would not be able to detect it. It sense the channel it is idle, but by that time actually somebody had started transmitting. See the problem.

(( )) sensing (( )) that where ever the (( )) if it is far also, it can sense (( ))

No it cannot. See the signal takes time to travel. Just remember that. May be for a large if you consider a very large network, it may be millisecond, right. So, in that millisecond, some station has already started transmitting signal on the line, it is sensing the line finding, nothing is there where signal has started from there has not reached here. See the problem.

So, the larger is the length of the channel, length of the medium, the more is the probability of the collision, and the more will be the degradation of the performance and that is one of the reason, one of the reason; there are many reasons from a first level course we will see. One of the reason; the length of the LAN is restricted by this, the propagation time. There are many other factors; we will find in a… Let us not waste, let us not spend time on that because we have many issues to discuss.

(Refer Slide Time: 05:22) ((No audio from 05:21 to 05:26))

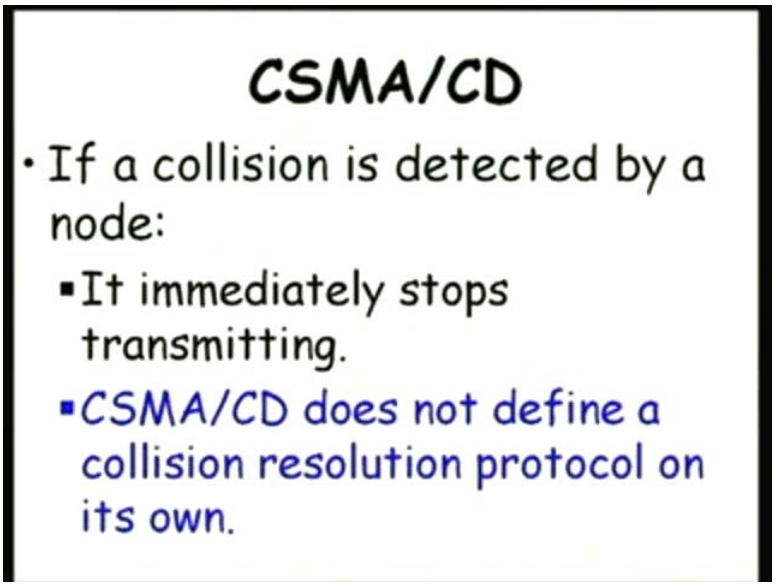


And once a node detects collision, I mean see this is the reason why collisions occur also. See the reason, we are saying that it takes time for the signal to travel and that is why collisions occur actually, because it will be extremely rare that two sources exactly transmit on the same time, same instant of the time. Because once a signal transmitted, the channel if it is found to be occupied; is busy, and then the others will not transmit, isn't it. So, where is the chance of a collision?

Let us assume that two stations do not generate or do not really start to transmit exactly on the same time in the clock sense that same let us say nano-second, if you are talking of a gigabit Ethernet. Let us say in the same nano second precision, they do not transmit. So, will collisions occur or not? Still collisions will occur because of this transmission delay. Is that ok?

((No audio from 06:28 to 06:34))

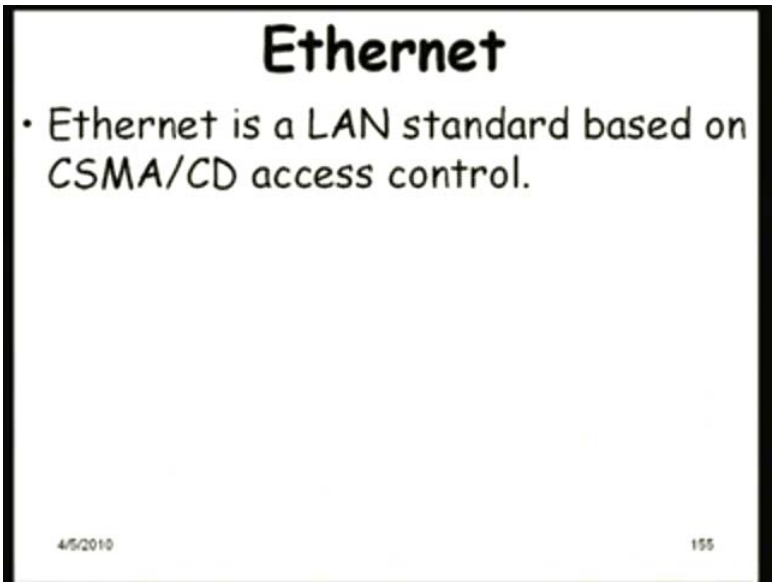
(Refer Slide Time: 06:34)



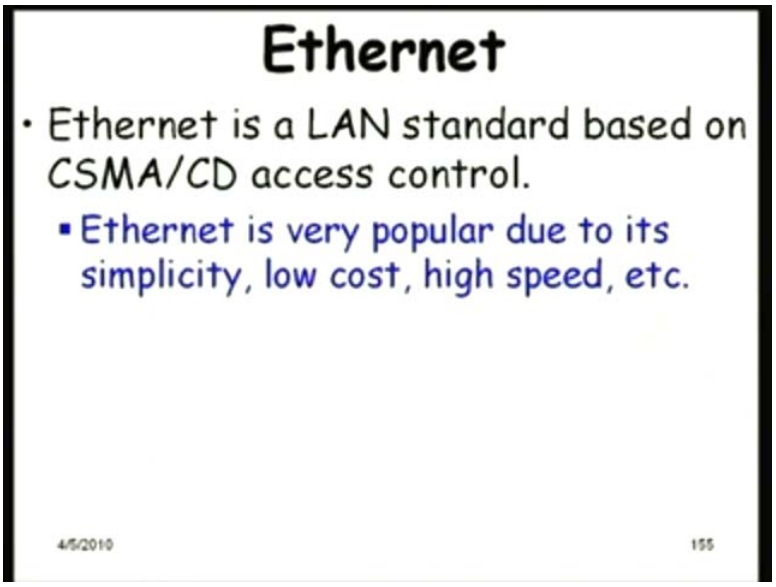
And from the first level course, you would know that the CSMA/CD does not define a collision resolution protocol on its own, where different implementations possible. For example, ethernet uses something and for example, can uses something.

((No audio from 06:50 to 06:54))

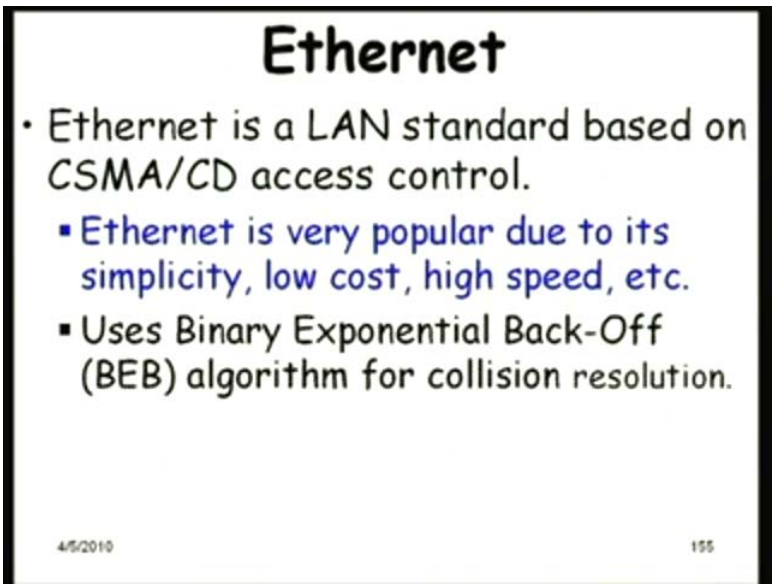
(Refer Slide Time: 06:54)



(Refer Slide Time: 07:01)

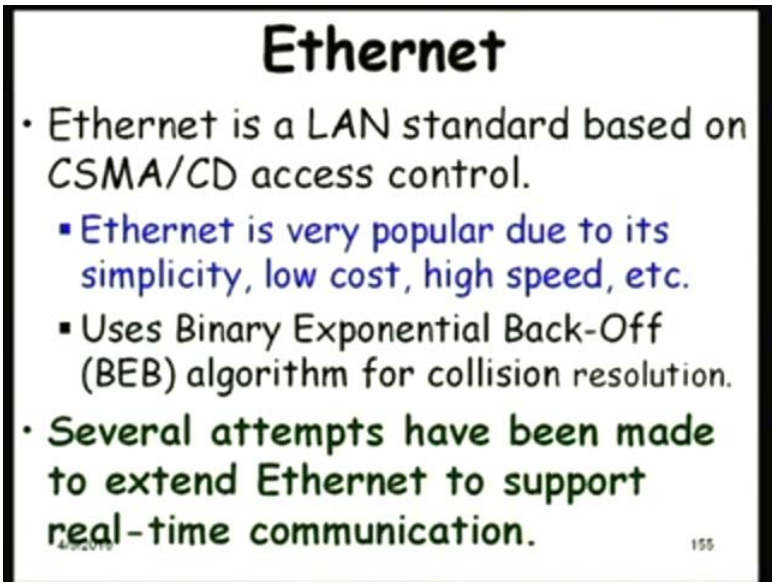


(Refer Slide Time: 07:04)



Ethernet is popular implementation of the CSMA/CD protocol; very popular due to simplicity, low cost, high speed. All of you know very well Ethernet from a first level networking course, uses the binary exponential back off algorithm for collision resolution.

(Refer Slide Time: 07:16)

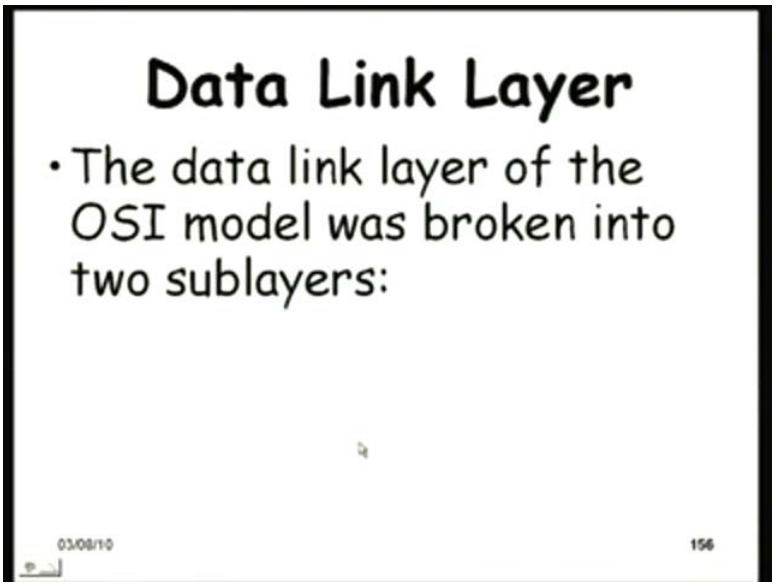


And since it is such a popular network present everywhere, every lab, every office; it is there and because of the uses to such a large number, the cost also has reduced considerably because of the sheer volume of the demand on Ethernet. It is very inexpensive; even as a hostel room you can set up a ethernet in few 100 rupees. So, naturally people are interested to use ethernet in real time application, but the basic problem here is that does not distinguish between stations. All are treated equal.

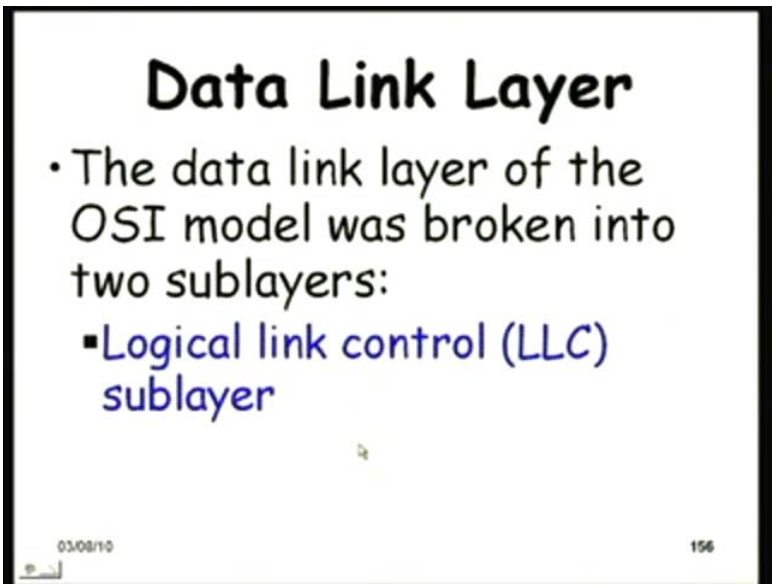
We will see some attempts that have been made to extend ethernet to support real time communication, and they are successful to various extents, but in some applications can be used. We will we will discuss this about two hours or so later.

((No audio from 08:19 to 08:22))

(Refer Slide Time: 08:22)

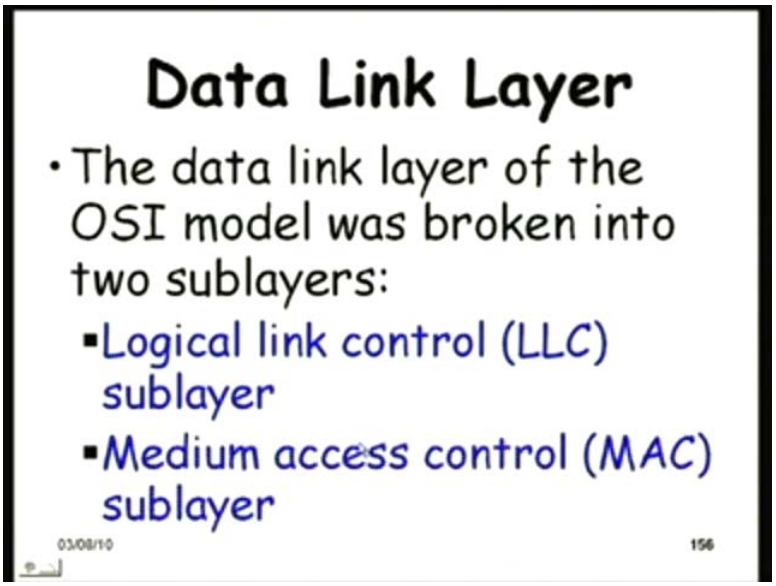


(Refer Slide Time: 08:27)



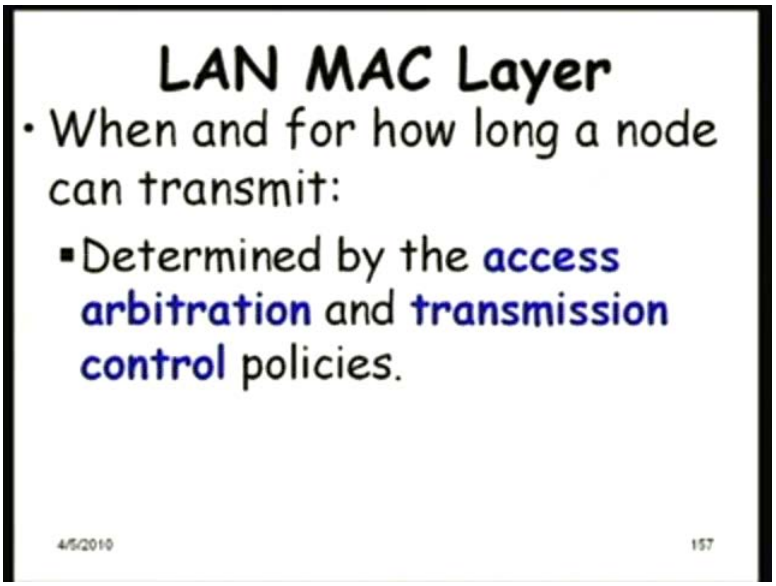
The data link layer is actually consists of two sub layers: the logical link control and the MAC sub layer, which we know from the first level course.

(Refer Slide Time: 08:31)



The medium access control; it implements the arbitration mechanism; which node will be allowed to transmit; its inbuilt into the MAC protocol.

(Refer Slide Time: 08:54)



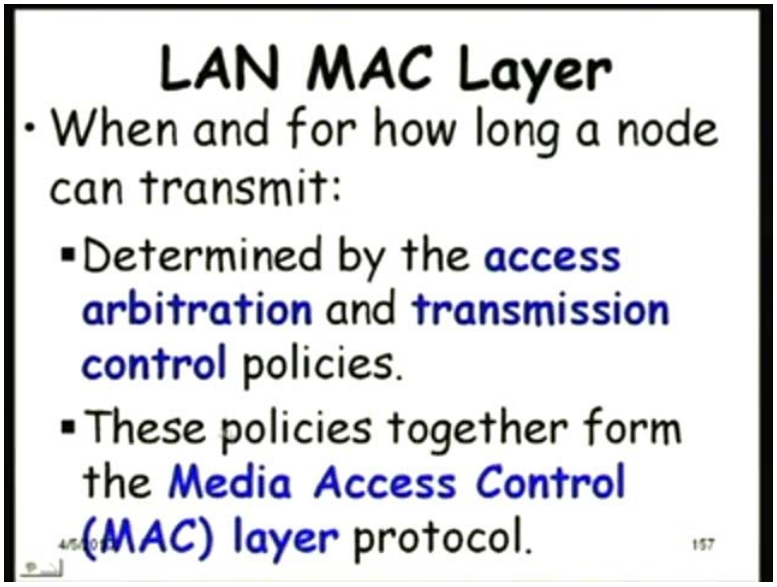
So, the MAC layer; ((No audio from 08:53 to 09:01)) it decides, the MAC layer is the one which decides for how long a node can transmit, and when it will be able to transmit. It is very important for a real time application because precisely we have to tinker here. We will have to manipulate this in a real time protocol; we are saying that ethernet is being also used for real time applications.

So, to adopt ethernet to real time application, we will exactly have to somehow control this, when exactly a node will able to transmit, which node will be able to transmit and for what period I mean how long it can transmit. Based on that we can you know deterministically say that when other data can be transmitted by the other nodes, right. Because we need that all real time data should be transmitted in the required time.

So, there are two policies inbuilt into the MAC layer. One is about when somebody can transmit. The other is how long. 'When' is decided by the access arbitration protocol. The access arbitration is when multiple nodes start to transmit, it decides, the access arbitration protocol decides who is eligible to transmit. The other should back off.

The transmission control policy on the other hand, decides for how long the transmission can occur. Once a node is allowed to transmit, for how long can it occur? It cannot just monopolize, and then all other nodes will miss out on their deadlines.

(Refer Slide Time: 10:54)

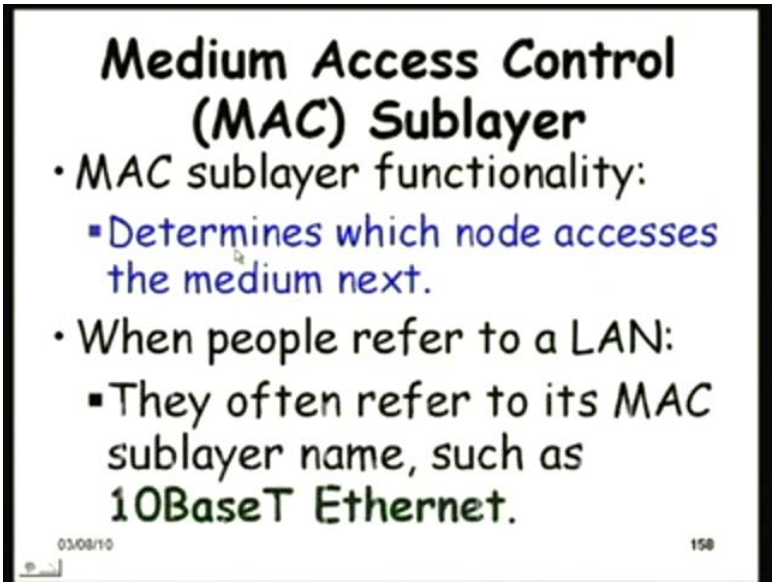


So, these policies together the access arbitration and the transmission control polices together, they form the medium access control layer, the MAC layer protocol. Several times as we proceed, we will fall back to this. We will be talking of the MAC protocol, the access arbitration protocol, transmission control protocol; I hope by that time, you will be able to recollect this.

(Refer Slide Time: 11:27)

This we had already discussed that a MAC layer; one of the work is to determine which node accesses the medium next, and typically when you talk of a LAN, you talk of a terms of the MAC protocol it implements.

(Refer Slide Time: 11:37)

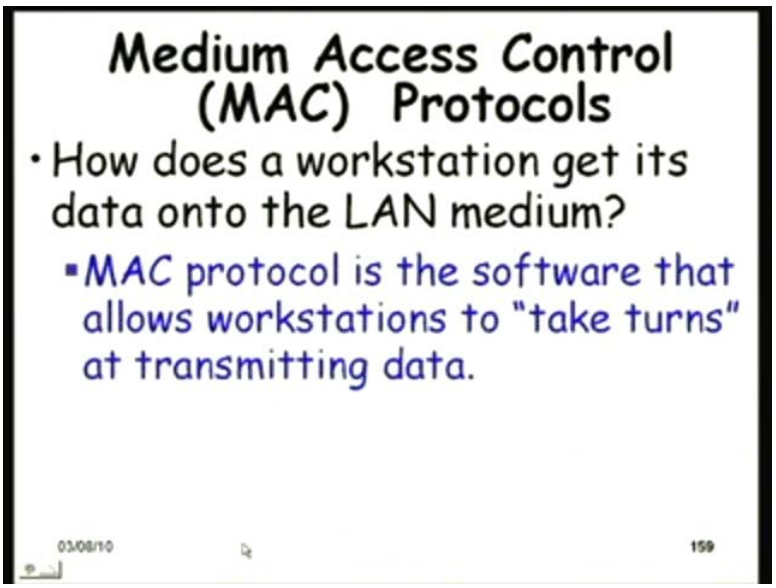


For example, if somebody asks that what kind of network you have in the lab, I mean in older times; now we do not have this in the lab. You will say that we have a 10 base T ethernet. So, that is the MAC protocol; the 10 base T ethernet is 1 type of Ethernet, right; that is, its MAC layer protocol is 10 base T ethernet.

(( ))

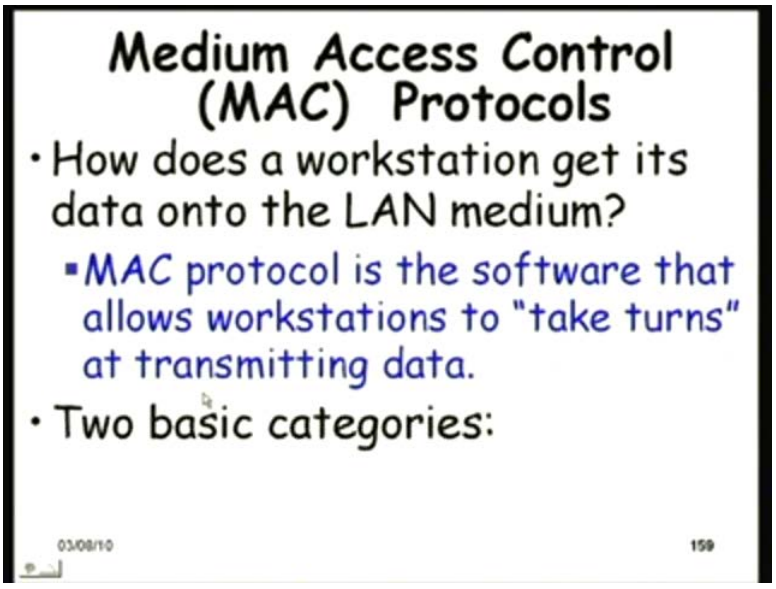
Yeah, we will just discuss about this 10 base T because such names we will hear and you will also hear, somebody will ask you what kind of network you have in the lab. So, we will discuss this term.

(Refer Slide Time: 12:36)

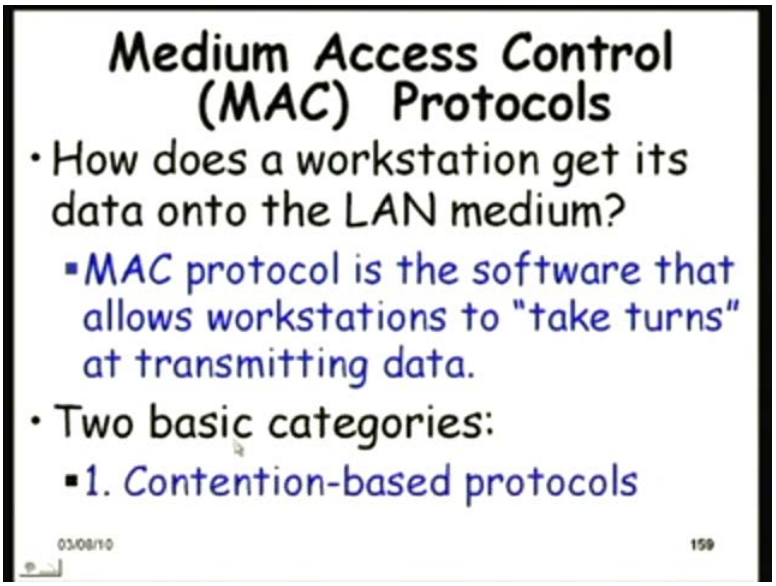


But how does a workstation get its data onto the LAN medium.

(Refer Slide Time: 12:54)



(Refer Slide Time: 12:58)

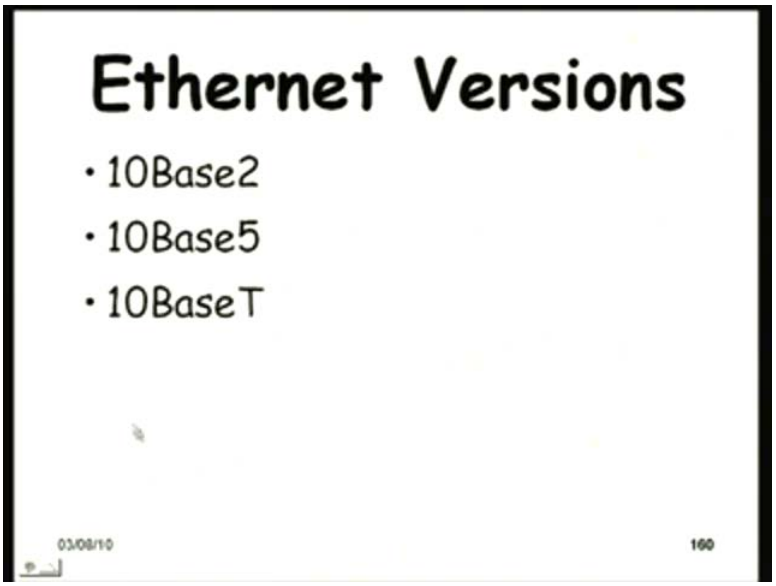


The MAC protocol is the one which decides which node workstation would transmit the data and then the terms are defined and they take turns in transmitting data, and based on what kind of protocol is used for the different stations to take turns in transmitting. Either we have a contention based protocol or we have a round robin protocol.

((No audio from 13:15 to 13:19))

So, these also you know from a basic course on networking. We are just refreshing those because we will use both this types of protocols in real time application. We will have real time protocols defined on the contention based protocols and real time protocols extended round robin protocols.

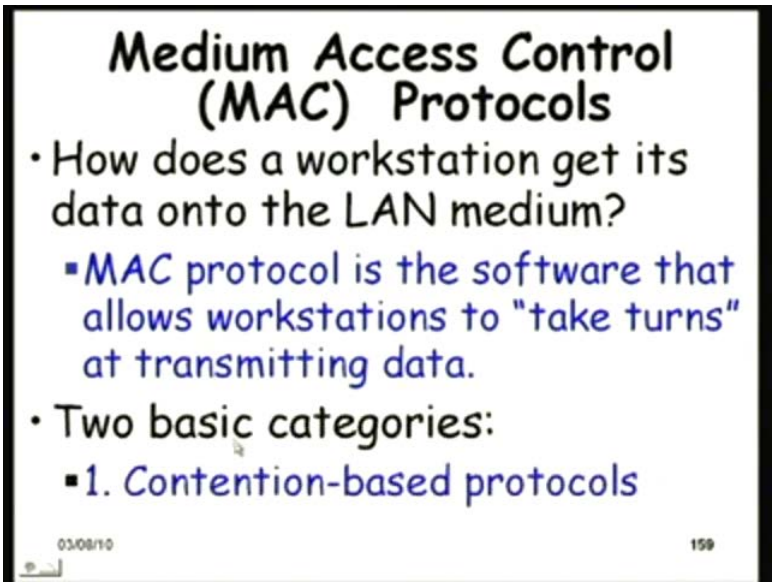
(Refer Slide Time: 13:48)



If you see the last 20- 25 years that the ethernet is an existence, several types of ethernets that have come in. 10 base 2, 10 base 5, 10 base T, 10 base F, 100 base T, or the First Ethernet, 1000 base T or the gigabit ethernet which we have in the lab now.

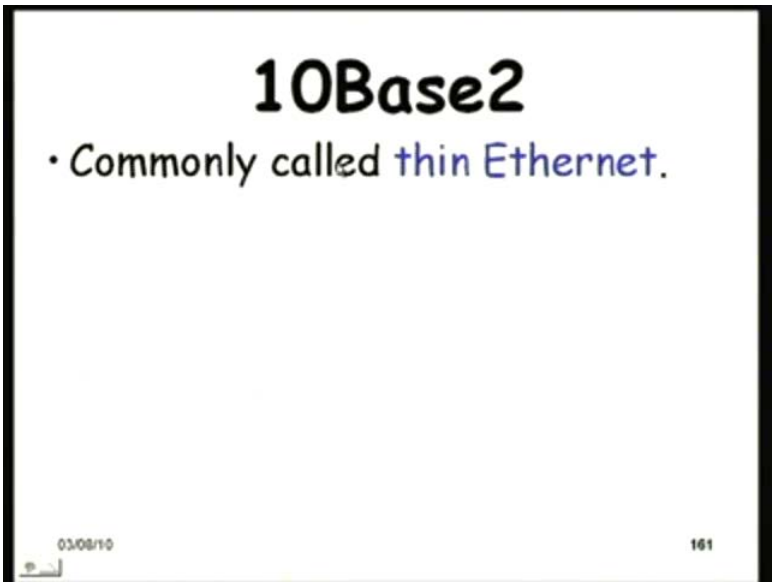
((No audio from 14:04 to 14:08))

(Refer Slide Time: 14:00)



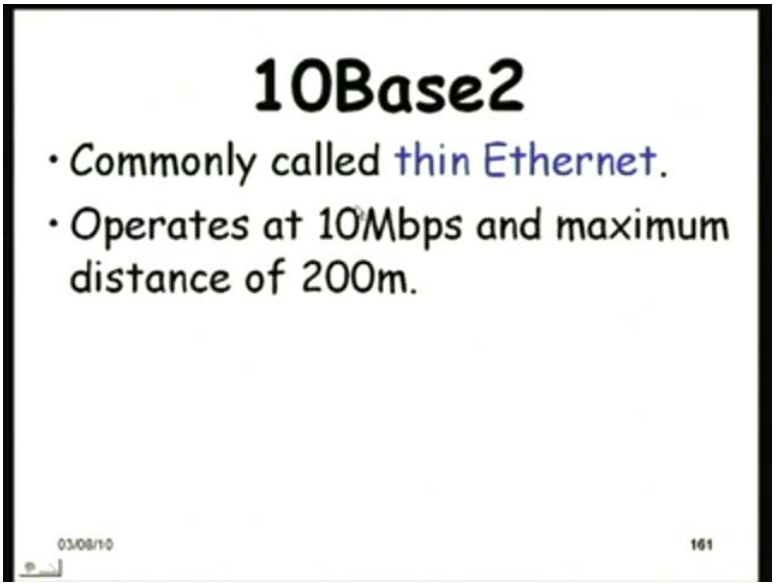
Let us see what are what do this mean. 10 base 2, 10 base 5, 10 base T, 10 base F, 100 base T, 1000 base T, etcetera; what do they mean, the numbers and so on.

(Refer Slide Time: 14:25)



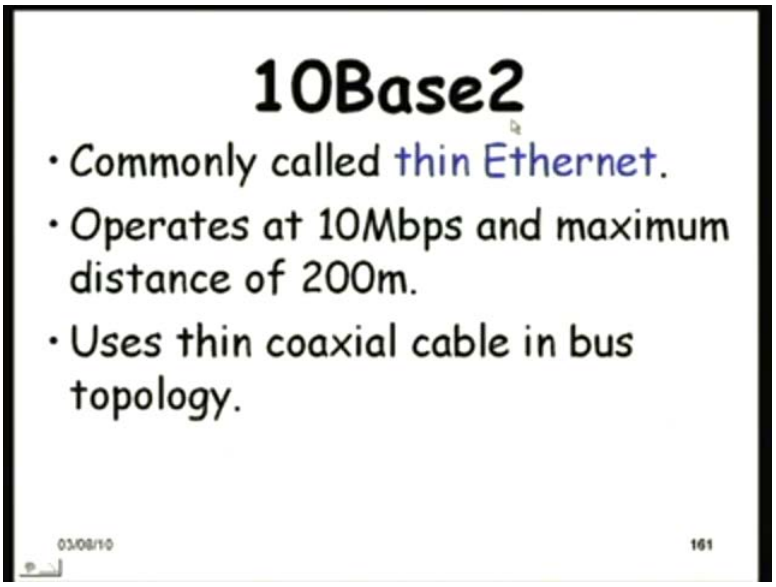
The 10 base 2 existed quite some time back, may be 15-20 years back. Those days it was called as the thin Ethernet. Now days nobody uses this, but old networks you can still find them.

(Refer Slide Time: 14:44)

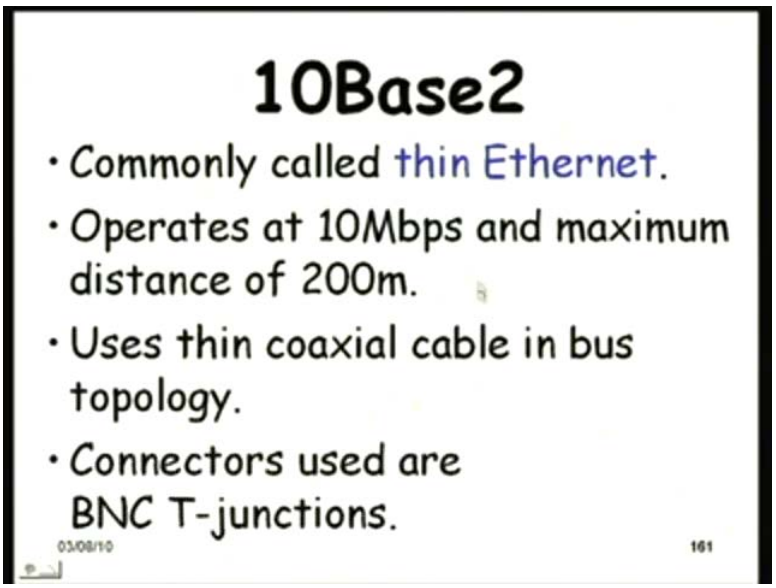


It operates at 10Mbps, 10 Mbps, and the maximum distance of this network is 200 meters.

(Refer Slide Time: 15:02)

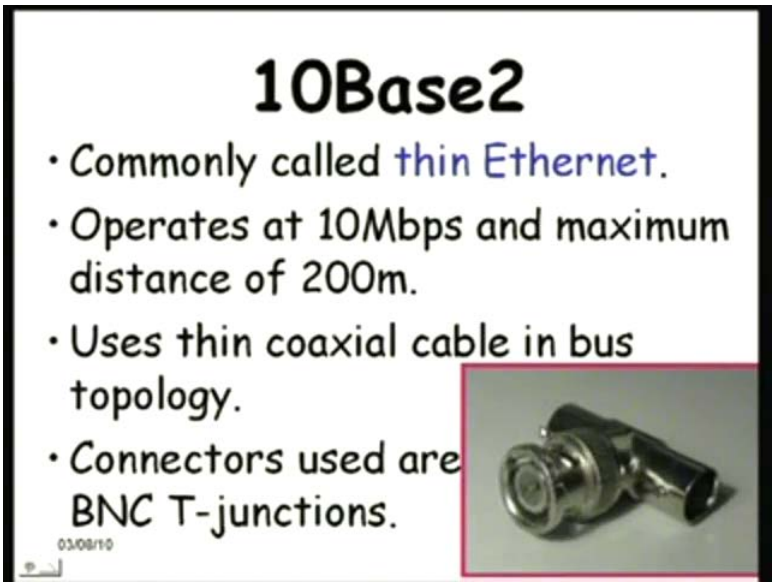


(Refer Slide Time: 15:07)



So, uses a thin coaxial cable in bus topology; we had seen the bus topology, the BNC-T junctions and so on.

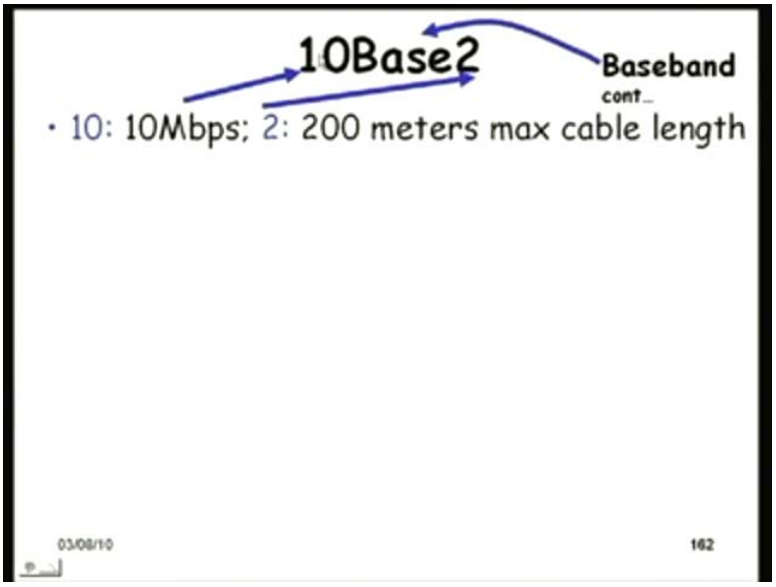
(Refer Slide Time: 15:15)



Used to be like this, the coax cable.

((No audio from 15:18 t0 15:21))

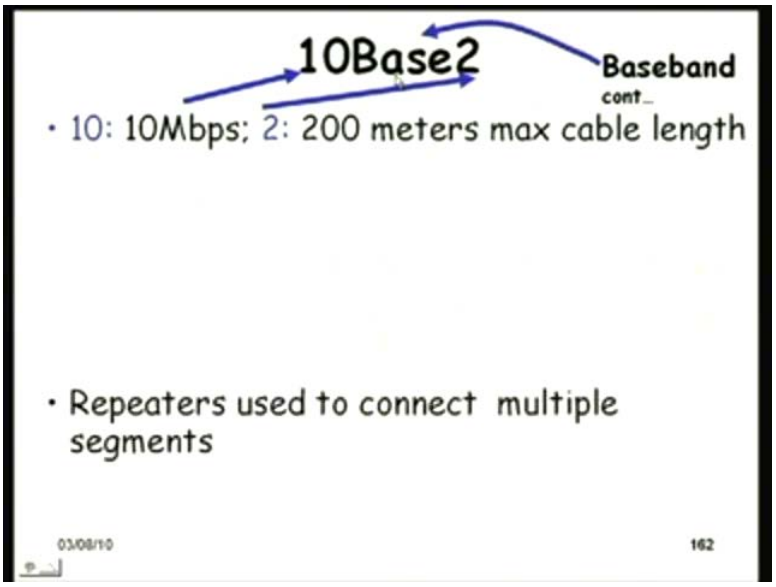
(Refer Slide Time: 15:21)



The 10 stands for 10 Mbps, 2 for 200 meters, and base for baseband transmission.

((No audio from 15:28 to 15:33))

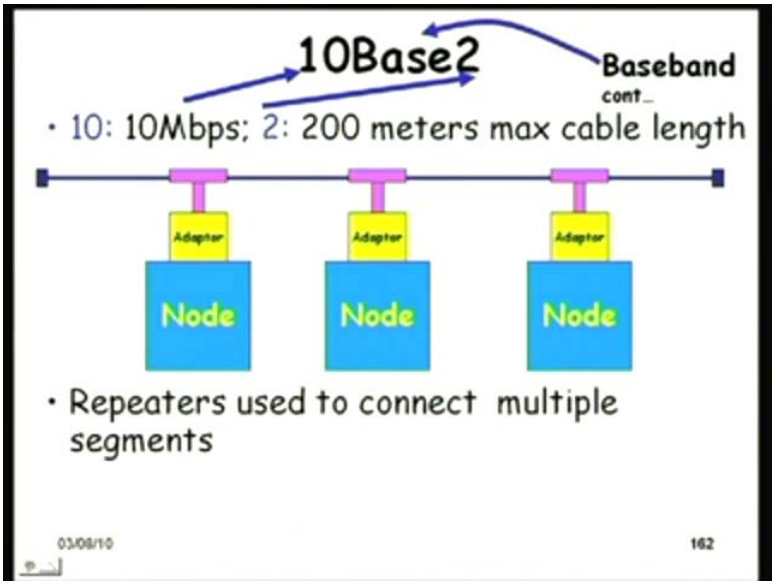
(Refer Slide Time: 15:33)



I hope all of you know what is a baseband transmission, how does it differ from a broadband transmission. So, the LAN transmissions occur at baseband.

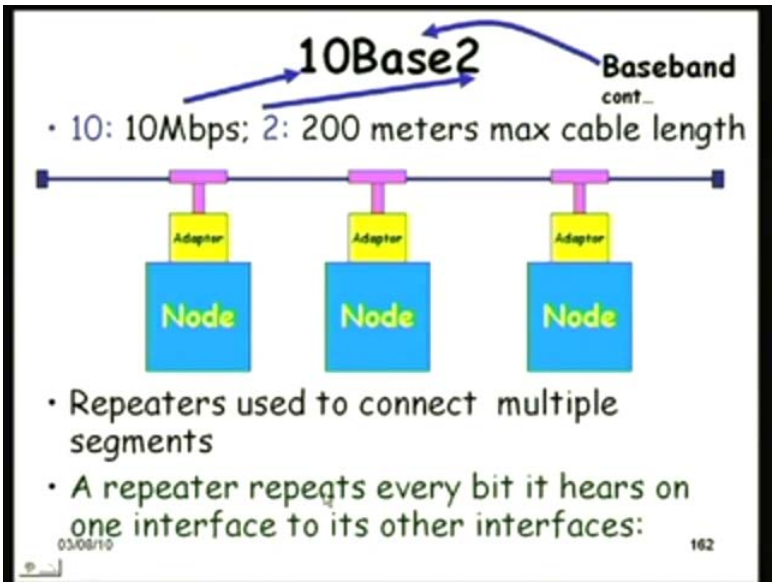
((No audio from 15:48 to 15:59))

(Refers slide time: 15:59)



The nodes are connected through a adapter which is a LAN card, a LAN adapter to the bus which is a coax cable, thin coax and T junctions terminated, but multiple segments, LAN segments can be interconnected using repeaters or hubs.

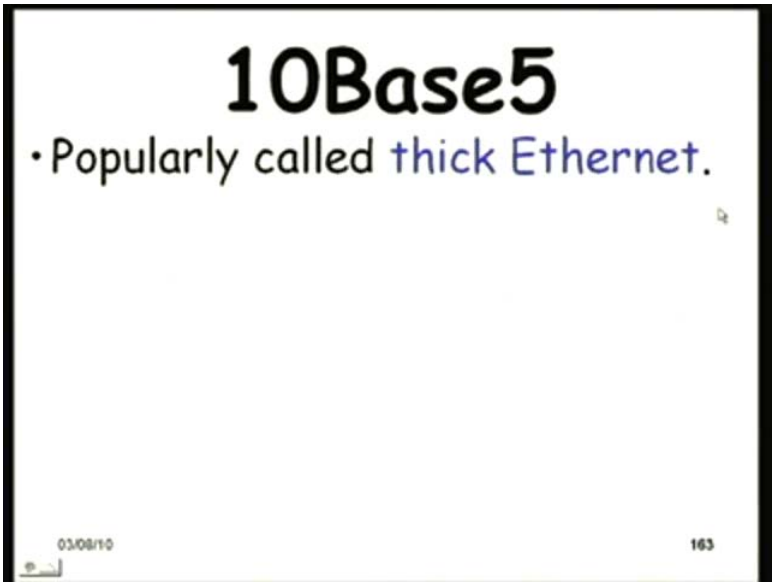
(Refer Slide Time: 16:31)



A hub would transmit every bit appearing on the bus to the other bus.

((No audio from 16:39 to 16:47))

(Refer Slide Time: 16:48)



And then we had the 10 base 5; it was called as the thick Ethernet, used a different type of cable and the transmission distance was 500 meters. But one of the reason we were saying is that the as the distance I mean the length of a LAN increases, the collisions become more and more. The probability of collision increases, right. But other than that

what restricts the length? I mean, we saw a 200, a thin ethernet is 200 meters, and a thick ethernet we are saying 500 meters. What restricts the distance? See this also the transmission is 10Mbps.

(( )) Because that is using thick cable. (( ))

So, how does that matter?

(( ))

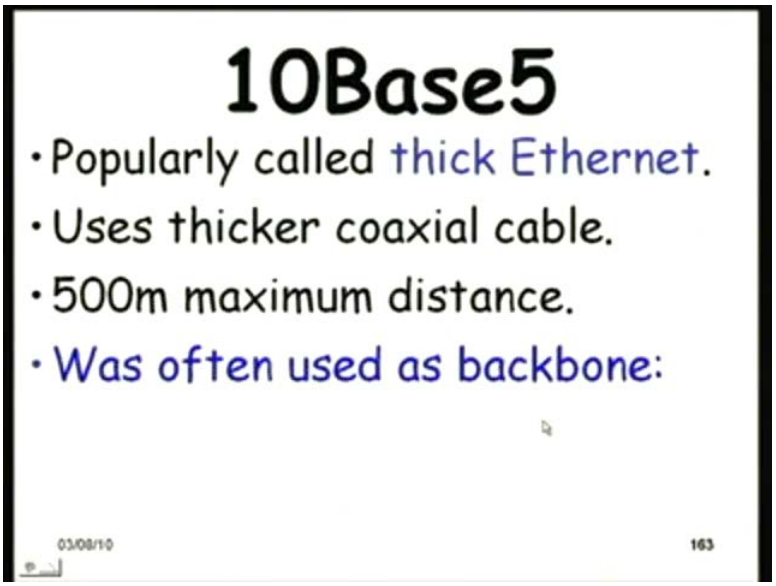
I mean what difference it makes, whether it is a thin cable or a thick cable.

(( )) Ok.

(( ))

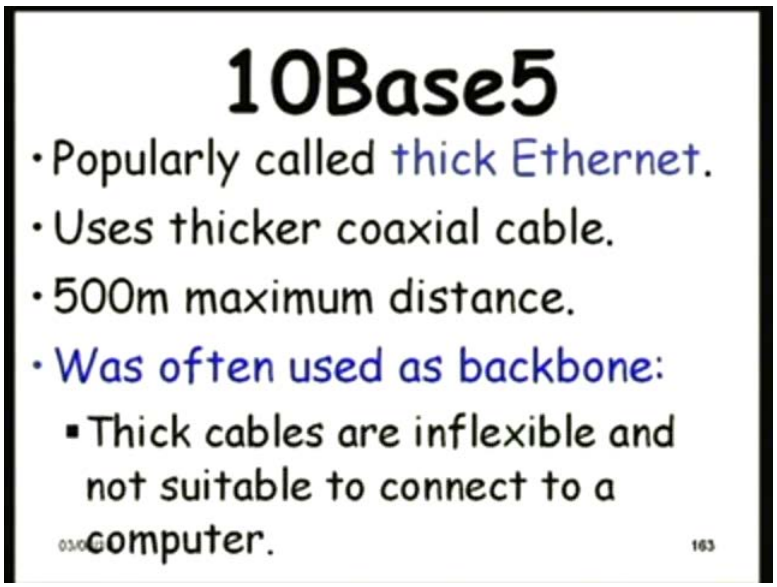
Signal attenuation; that is a major problem that restricts the length of a LAN segment. So, that is what he says that attenuation will be more in a thin coax cable compared to a thick coax cable, and that is the main reason why this one is 500 meters, other one is 200 meters. But again, when the cable is too thick, we cannot; it is very difficult to use. So, the thick ethernet was rarely used in lab situation.

(Refer Slide Time: 18:37)



It was used as a backbone. In the lab situation, it was the thin ethernet which was popular. The thick ethernet was used as the backbone to connect different LAN segments.

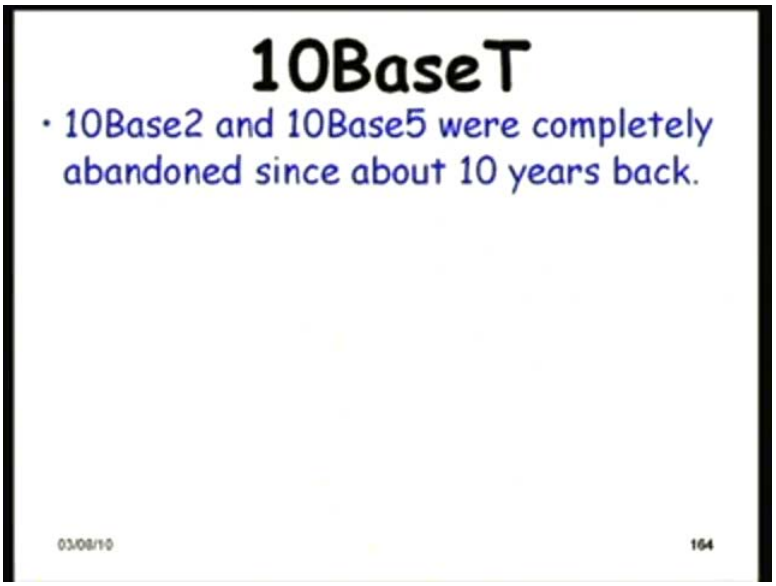
(Refer Slide Time: 18:46)



The thick cables were inflexible and not really suited to interconnect a computer. You know how do you thick cable, how do you attach to your computer.

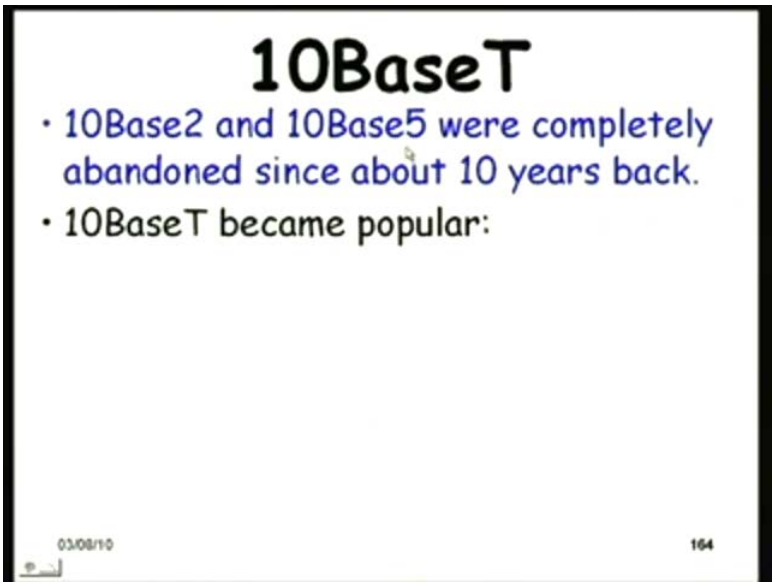
You cannot really bend it and so on; whereas, a thinner cable is much easier to interconnect. So, the LANs used to be thin ethernet, and then the interconnection between the LANs used to be thick ethernet.

(Refer Slide Time: 19:20)



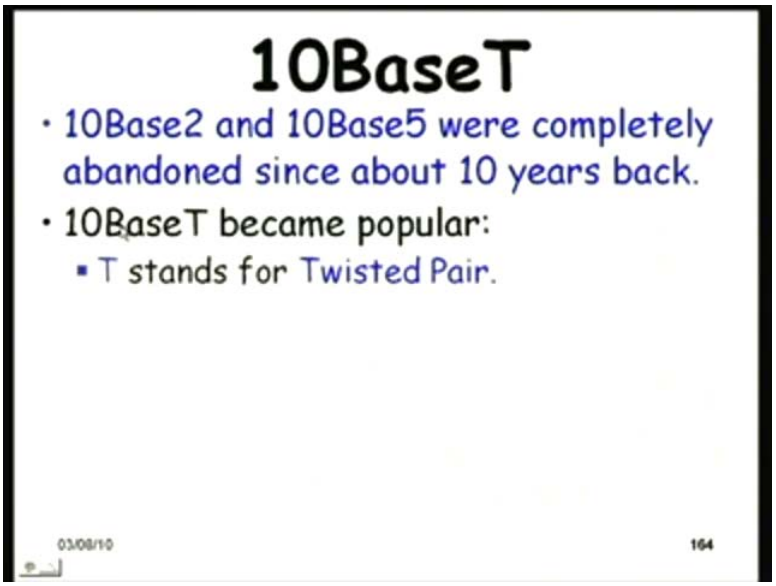
And then, we had the 10 base T. About 15 years back, 15 years back, the 10 base 2 and 10 base 5 were completely abandoned.

(Refer Slide Time: 19:36)



Suddenly the 10 base T became popular. It suddenly vanished actually, the coax cable within a year refined that nobody is using a coax.

(Refer Slide Time: 19:47)



Here T stands for twisted pair. Why to twist the wires?

(( )).

I mean how does that reduce the electrical interference?

(( )) there is a noise on the (( )) Ok.

(( )) Ok.

(( ))

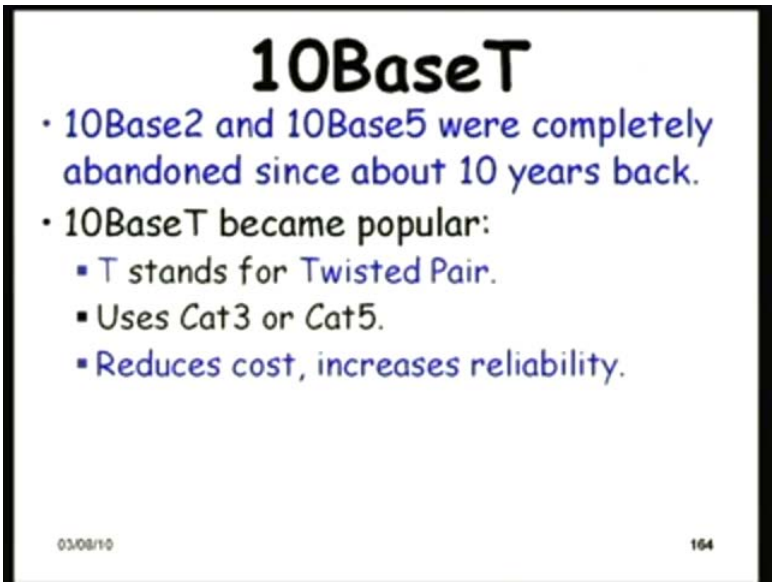
Yeah exactly. So, if they are tightly twisted, then similar noise will be induced on both the wire, and then the signal, the common mode, I mean the common mode noise can be eliminated and the signal can be will not be affected by the noise. Yes that is the idea.

And then, the cat 3 and cat 5 wires were used for 10 base T in the subsequent years. First cat 3 and cat 5. What is the difference between a cat 3 and a cat 5 wire? Cat basically a category, isn't it. Category 3 and category 5.

Cat 5 has more turns per square per centimeter, tightly twisted. That is one thing, but then we will see that the number of wires inside is also different number of struts, that is also different. So, some type of network you can implement at cat 5 which you cannot;

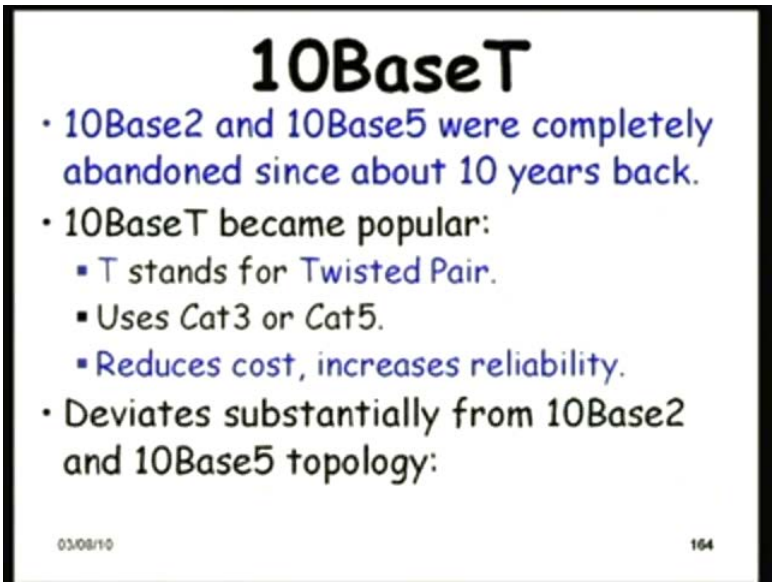
those protocols you cannot implement on cat 3 because the wires are different. We will just see that.

(Refer Slide Time: 21:38)



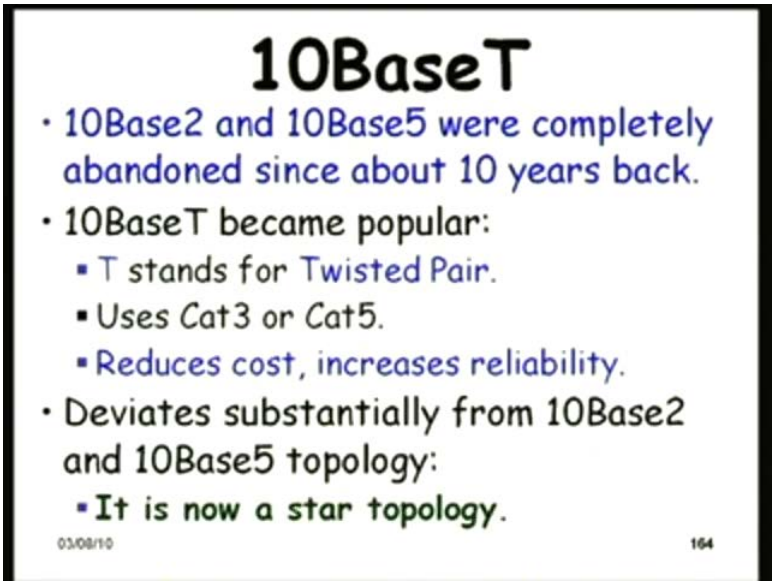
The twisted pair suddenly became popular because it reduced cost and at the same time increased reliability became a star connection in no time. I mean one year you find that the labs are setup using a bus, next year you see the absolute use a star connection to setup your lab, and use twisted pair in the at much reduced cost. So, and not only that very increased reliability. One wire has problem, still the network operates only one computer is not working change the wire it will work.

(Refer Slide Time: 22:16)



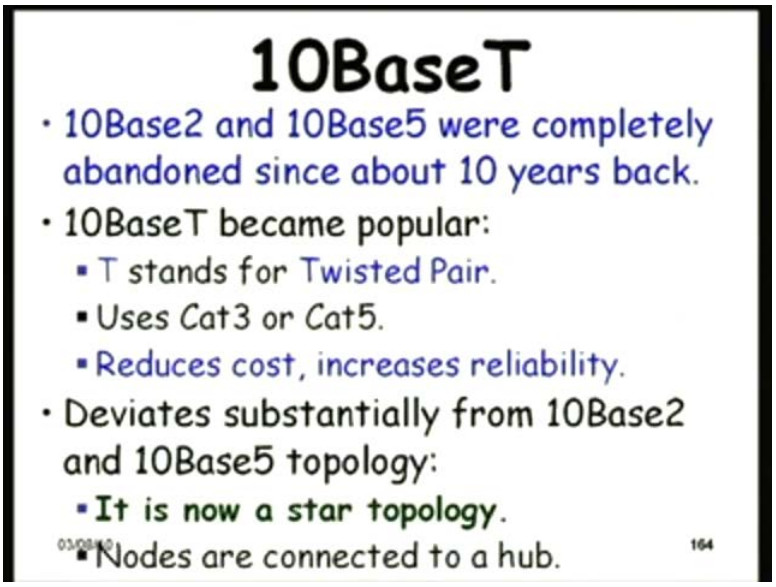
Deviates substantially from the base 2, 10 base 2 and 10 base 5 topology.

(Refer Slide Time: 22:22)



Became a star topology from a bus topology.

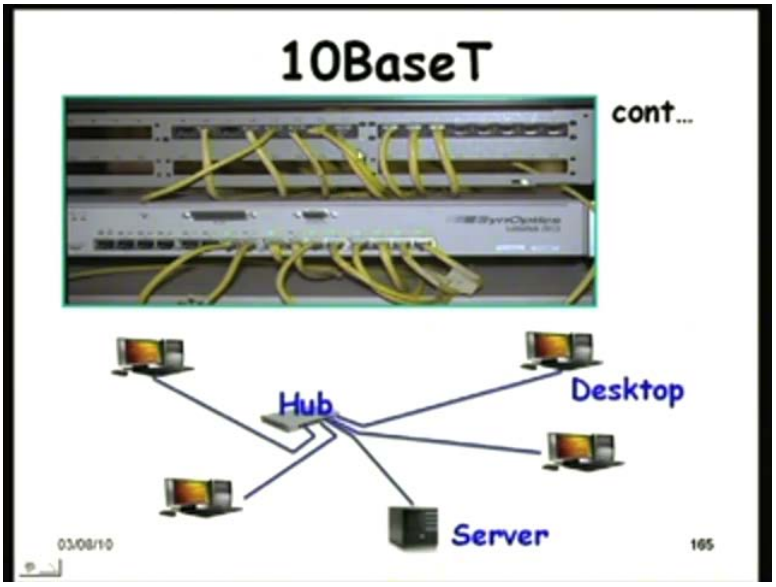
(Refer Slide Time: 22:26)



Sudden change in the topology and the nodes were connected to a hub.

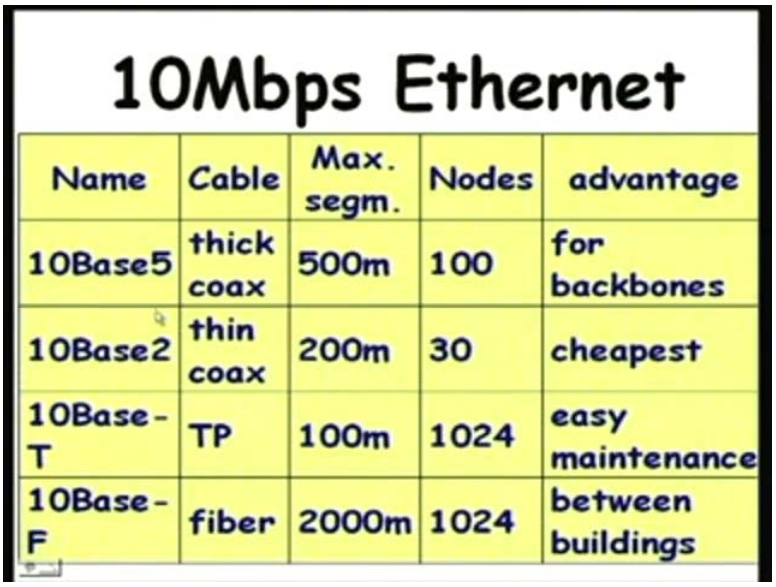
(Refer Slide Time: 22:32)

((No audio from 22:32 to 22:39))



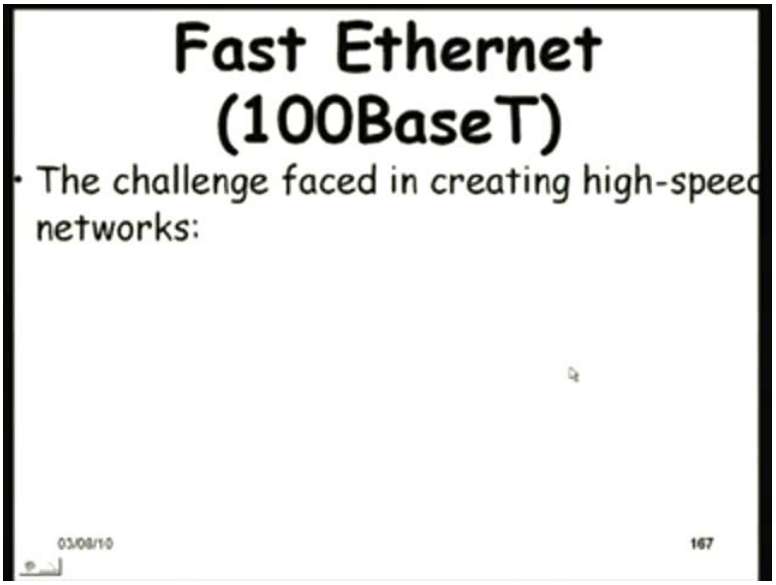
So, to the hub; the connections from different computers were attached and it appeared something like this. This is the hub, then the computers where all attached to it form of a star network.

(Refer Slide Time: 22:57)



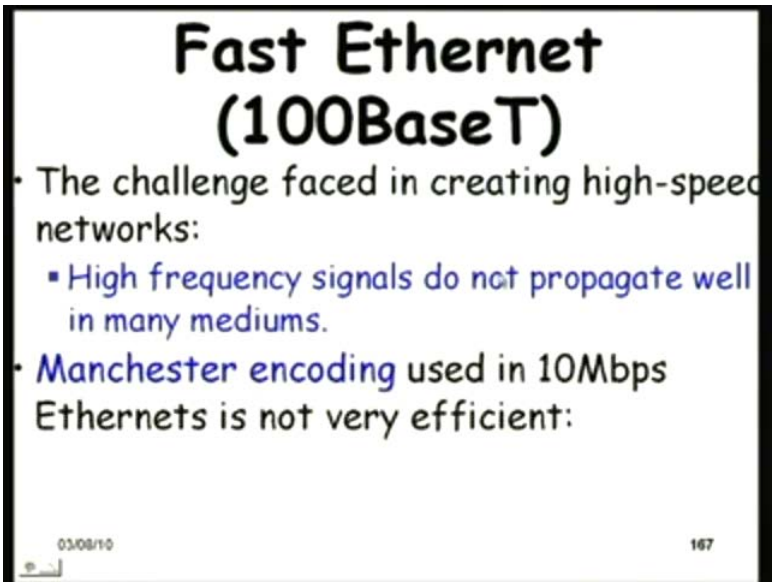
If we compare this different network, the 10 base F was based on fiber. Naturally the distance of the network is larger and the number of nodes that can be attached to it is also larger because each node sinks some signal, isn't it, as it listens to the noise; sorry listens to the signal, it sinks some signal from it naturally. A ten base F will have many more stations attached to it; typically used between buildings inflexible. 10 base T also you can attach large number of nodes, easy maintenance.

(Refer Slide Time: 23:58) ((No audio from 23:52 to 23:58))



And then we had the first ethernet which appeared around I think 10, 8-10 years back.

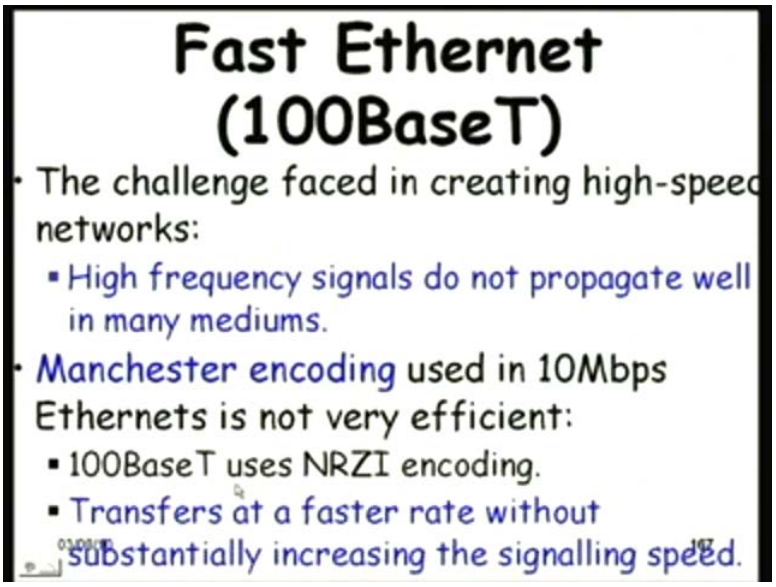
(Refer Slide Time: 24:09)



The computers became faster, internet had come in, and there was need for letting the computers operate transmit at a faster rate, but how can somebody transmit at a faster rate on the same twisted pair? Again, a twisted pair, the kind of noise etcetera; see basically the signal rate is restricted on how much noise is getting induced, isn't it. As the signal rate increases becomes gigabits and so on, little bit of noise also can create problem.

So, it is the same twisted pair. So, how is it that able to transmit ten times the speed? The reason is that a different encoding was used in the 100Mbpsnetwork, that 100 base T used the NRZI encoding compared to the manchester encoding, the older encoding in the 10 Mbps.

(Refer Slide Time: 25:15)



So, the data transfers could occur at a faster rate without substantially increasing the quality of the medium or the signaling speed of the medium, without substantially making difference to the medium to transmit at a faster rate because of a different encoding used to transmit the signal where it is more noise proof.

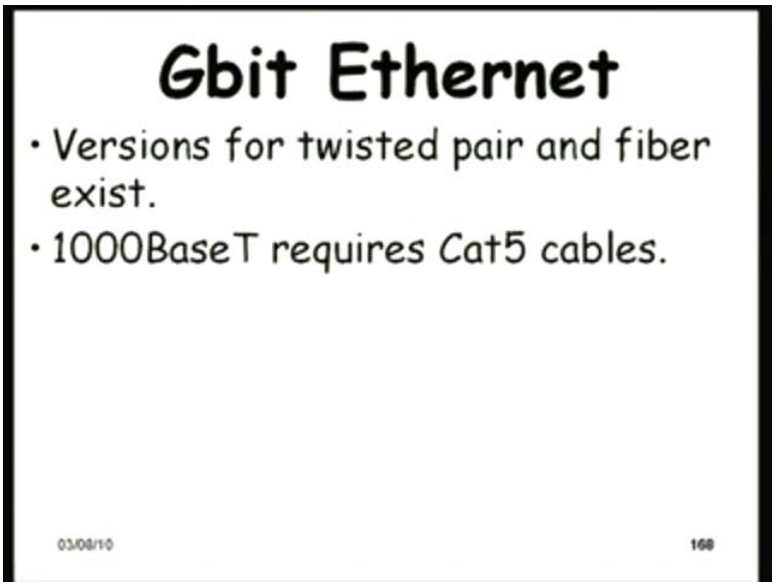
((What does the))

(( )) return to 0, I do not know we will have to look up.

(( ))

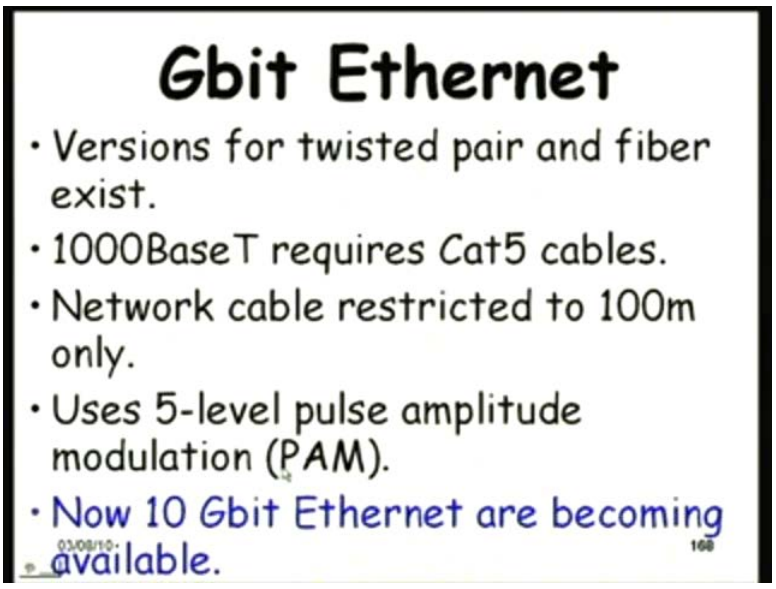
Inverse. Its name of a encoding scheme. You can find it on any book or just search on the internet, you will find that. And then we have the gigabit ethernet now present in the labs.

(Refer Slide Time: 26:14)



There are two different versions; one using the twisted pair, another using the fiber. The gigabit ethernet is also referred to as 1000 base T. All these ethernet transmissions are baseband transmissions. Just remember that. It requires a cat 5 cable. We will see why cat 5 cable. 100 meters only uses a 5- level pulse amplitude modulation.

(Refer Slide Time: 26:50)

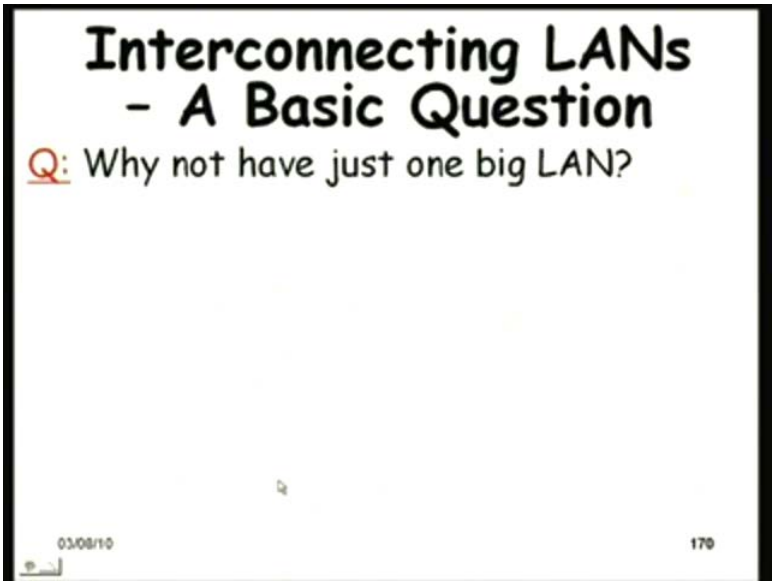


So, again the modulation changed, and that is partly the reason why signals could be transmitted at a faster rate, and now we have 10 gigabit ethernets are available.

(Refer Slide Time: 27:16) ((No audio from 27:11 to 37:16))

So, this cards take care of transmitting gigabit, can be attached to the gigabit network.

(Refer Slide Time: 27:26)



I think the answer is to… We are just answering trying to answer some questions, isn't it. What was it? I mean how it could become gigabit ethernet without and why does it run on cat 5 alone, right? Why not on cat 3 a gigabit ethernet?

So, we do not have the answer right now here on the slides, but the answer is something to do with the protocol and the full duplex transmission that became possible. The full

duplex transmission, we will just see shortly, and at the same time a station can both receive and transmit. It was restricted to only receiving or transmitting. We will just look at that issue now. I mean shortly afterwards, and two pairs of wires were needed for the protocol. Naturally when a full duplex communication, you need two pairs of wire, isn't it. So, we will just see that exactly.

So, we will just look at that, but since we will be discussing later quite widely on LAN inter connections in real time communication, we will also answer a few basic questions, address basic issues in LAN inter connection.

One question is that why not just have a big LAN? What is the advantage of, first level knowledge first level networking knowledge that is. Why not have one big LAN. Why do you know have one LAN in one lab, you know you have some three four labs in the department, separate LANs there and then inter connect them. Why not all of them in the same LAN?

(( )).

Why not cost effective.

(( )) connect the whole thing with the same type (( ))

You mean cabling cost, cabling cost. No, cabling cost is not much. Twisted pairs anyway do not cost much.

Reliability.

How it is reliable, I mean how by making it…

A link is broken net or network will be failed (( ))

No, in a present day star connection, it one link broken does not bring the network down. Sorry.

(( )) Complex physical structure.

Why complex physical structure? You can…

(( )) cables of different lengths.

Cables of different lengths, does not matter. You can always attach cables of different length.

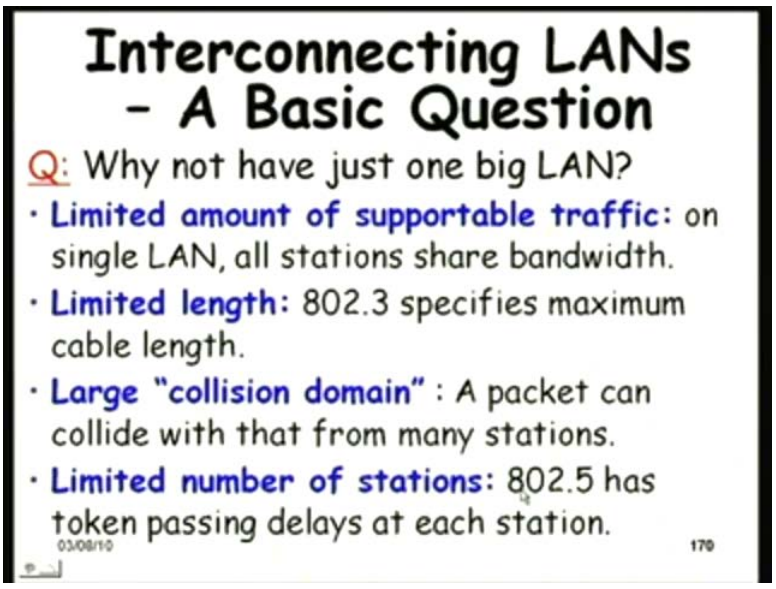
(( ))

That is what he said know, link fails, but I was saying that link fail does not bring the network down. You know a link failed and you just replace that link. ((Easy to debug)) Why easy to debug? There also see when you have a large LAN found that computer is not working, you know that something wrong with the link. Here also same thing, when there are multiple LANs, found one computer not working, look at the link. Because It is a star connection. Just remember, they are not bus connections.

(( ))

No not really. So, let us see. The reasons why we need to separate large lab into smaller labs.

(Refer Slide Time: 31:17)



One is that in a single LAN, all stations share bandwidth. If you put hundreds of them, the chances of collisions will be too much, and the throughput will reduce drastically because you know they are in a broadcast mode, and any node can disrupt traffic from

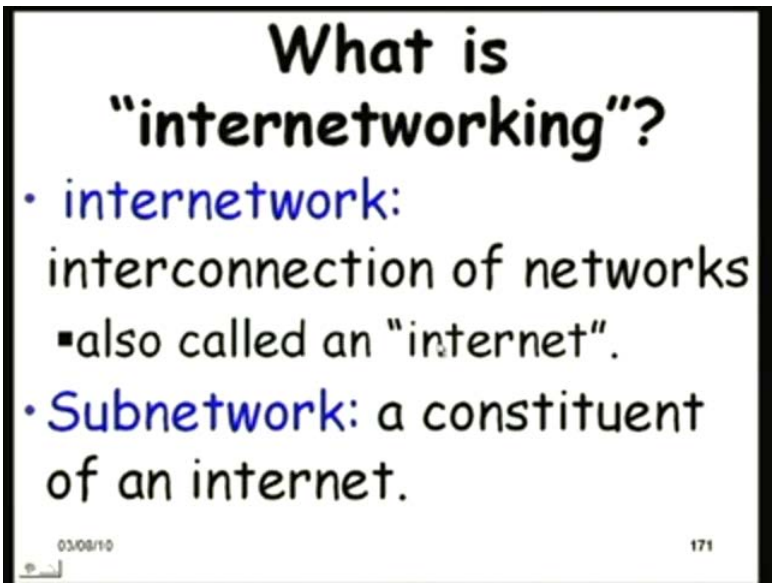
another node, right. They contend for the same channel and every LAN supports a limited amount of traffic. So, this is one major reason that when you separate them into inter connected LANs, it becomes much easier for computers to communicate without a performance degradation.

Second reason is the length restriction on the LAN. A single LAN, we were just mentioning that there are several reasons; while the length is restricted the cable length is restricted, large collision domain.

So, these two points; the first point and the third point are slightly different. The first point says that if each LAN supports let us say 10 Mbps or 100 Mbps, then five of them will support 500 Mbps traffic same time whereas, if it is just one large LAN, at best it can support 100 Mbps. The collision domain in large LAN, the collision domain is large, and any node can collide with any other node. Here we are restricting the nodes with which it can contend. And not only that. The different LAN protocols, they limit the number of stations that can be attached and also in the token ring architecture, you have delays at it is station that occurs.

So, it becomes if you have too many stations in it in a token bus or a token ring, then by the time a station gets its turn, it may be too late for a real time application.

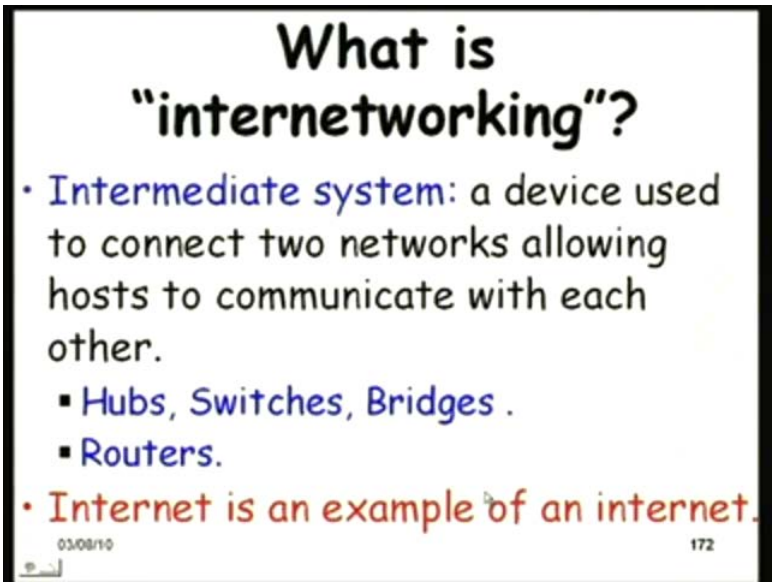
(Refer Slide Time: 33:57)



So, this we know that we have network of networks. Small i internet and capital i internet, we know that the difference, isn't it.

Small i internet is any two connections of networks whereas, as if it is a capital i internets denotes one specific instance of the internet. See if we have one LAN here and another LAN in the other room, you can just interconnect them and we have a small i internet. But the capital i internet denotes to one specific network on which the World Wide Web is hosted, and then the parts are the sub networks.

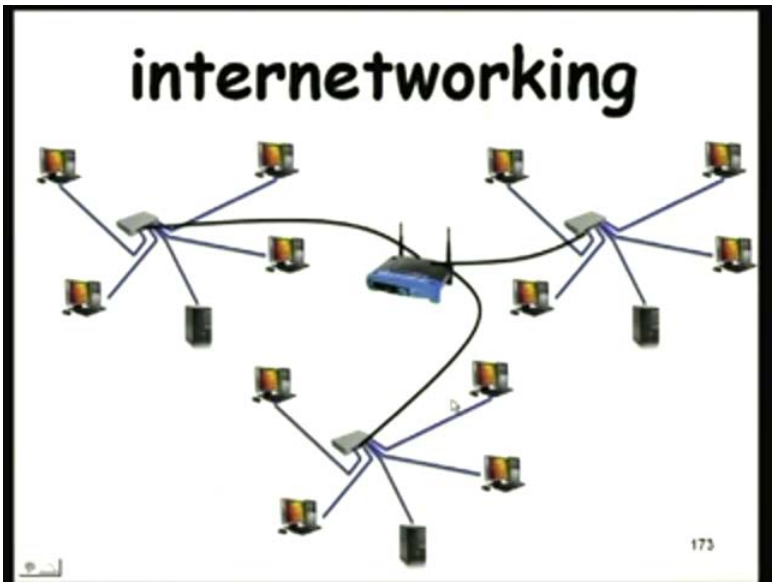
(Refer Slide Time: 34:45)



Various devices are used to inter connects the networks; hubs, switches, bridges; you know then the routers, we will not spend time on that.

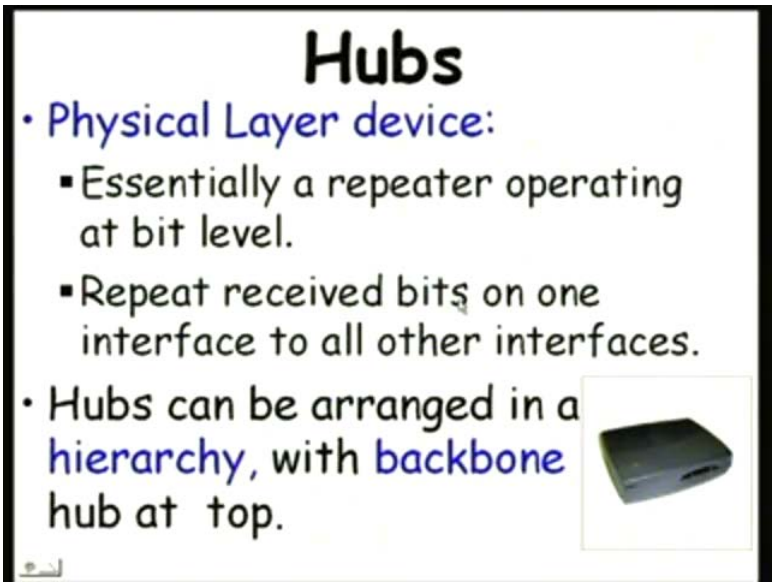
We can say that capital i internet is an example of a small i internet or is a specific case of a small i internet. We will just spend couple of minutes in reviewing the internet working.

(Refer Slide Time: 35:16)



So, this is a typical situation where we have interconnected some LANs using a router or a switch.

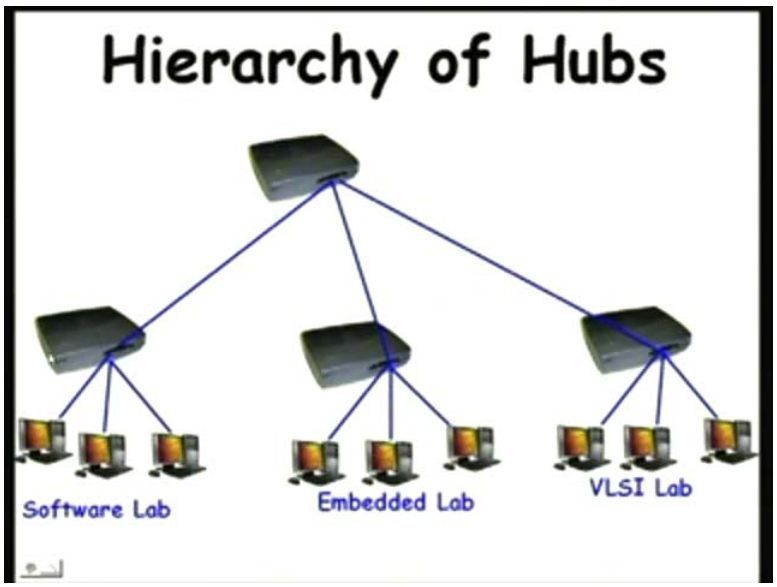
(Refer Slide Time: 35:28)



We have hubs and inter connect, inter connected them using a switch. Hubs you know that is a physical layer devices, repeat every bit, operate at the bit level. They do not understand addresses etcetera. Just whatever bit they appears on the line, they repeat it in all interfaces.

Available as we were saying, very inexpensive; few hundred rupees, can find in the market, arranged this can arranged in a hierarchy with a back bone hub at the top, can be configured like this.

(Refer Slide Time: 36:12)



You have different labs here, adjacent labs in each one has a hub, and then inter connected in a tree configuration with a hub at the route. ((No audio from 36:30 to 36:40)) So, here the need for the host to detect a collision limits the size to five hubs for 10 Mbps ethernet and three hubs for 100 Mbps ethernet. Do you agree with this, that for a 10 Mbps ethernet you can have five hubs inter connected in a tree hierarchy, for 100 Mbps ethernet you have three hubs. Why is that, and the answer we said is that to be able to detect a collision, do you agree with this? ((No audio from 37:19 to 37:25))

See here 5 for 10 Mbps and 3 hubs for 100Mbps. That can be inter connected ((No audio from 37:35 to 37:40)) in a tree actually.

So, why is that? So, this is the size of the hierarchy or the depth of the hierarchy. I am not saying the total number in the hierarchy, sorry total number of hubs that can be interchanged. The one that we are saying size is actually the depth of the tree.

((No audio from 37:48 to 38:00))

(( ))

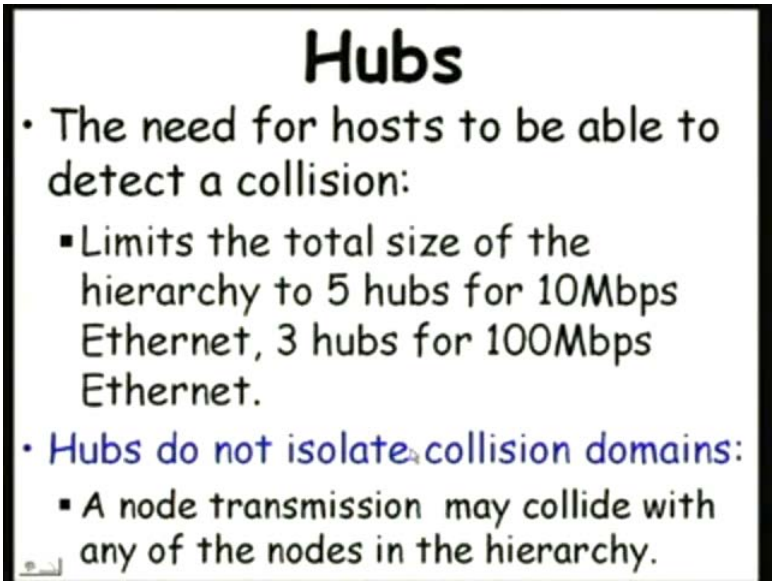
Exactly.

(( ))

Yeah that is based on what we discussed few minute back; is about the propagation time because each LAN we know that it is 100 meters. So, if five of them are there, the depth is 5. So, the transmission from one to the other, the other extreme will be 1000, isn't it, 5 and 5. So, for that, it is a 1000 meter it becomes. So, at a lower signaling rate, 10 Mbps can still mange with 5, but as the signaling rate becomes higher, it is too much, 10 hubs is too much.

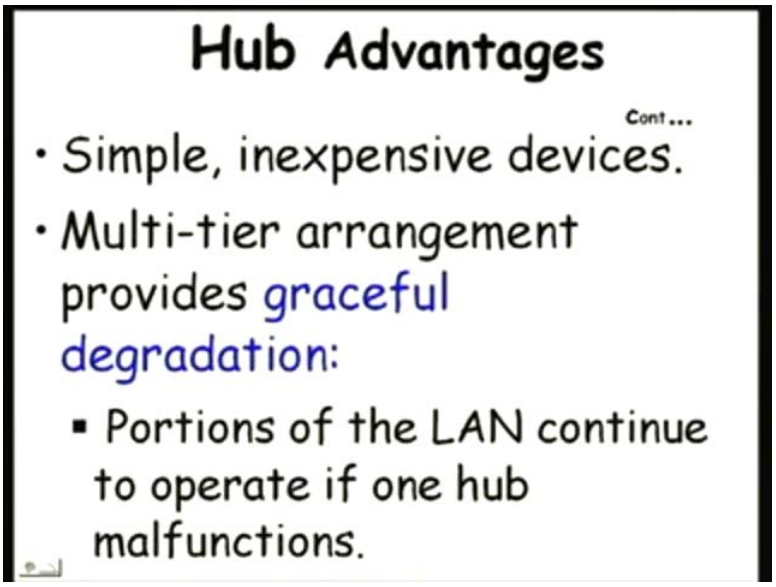
So, again the answer is based on what we discussed couple of minutes back. The propagation delay and how the collision is can occur, the chances of collision is more if the length of the medium is more etcetera. The answer is in this the same thing here, right is that ok?

(Refer Slide Time: 39:16)



But one problem with such a tree of hubs is that they do not isolate collision domains. The transmission from any node can collide with transmission from any other node in the hierarchy. So, as the depth becomes more and more, computers get attached, there will be performance degradation.

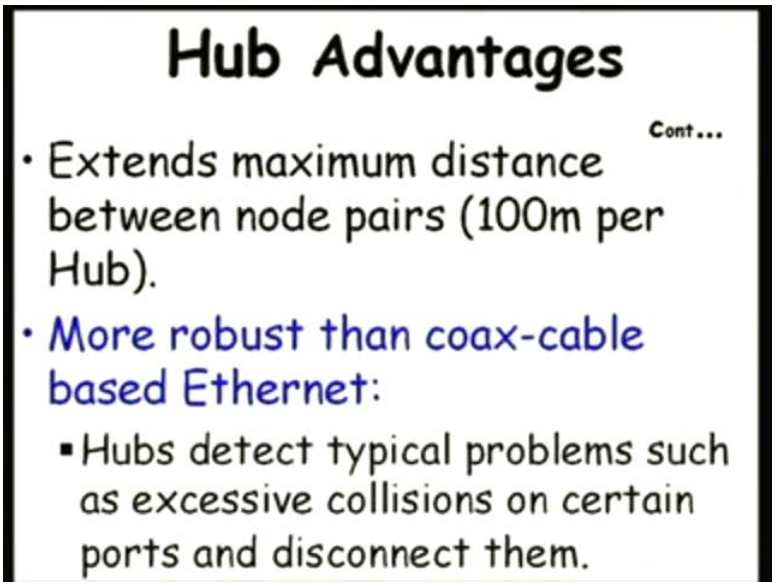
(Refer Slide Time: 39:46)



But simple as we were saying couple of 100 graceful degradation, some part gone, still does not matter, it will work. Portions of the LAN continue to work even if one hub malfunctions. Many advantages are there.

((No audio from 40:03 to 40:16))

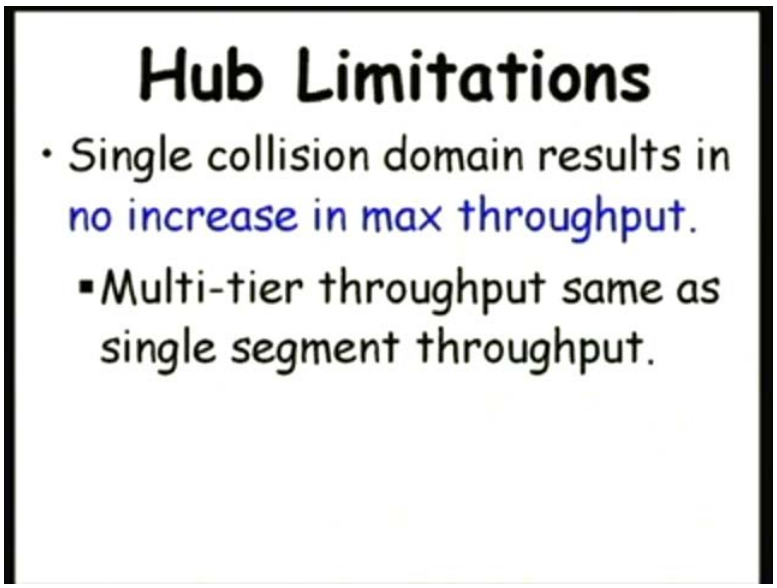
(Refer Slide Time: 40:03)



Its more robust than the coax cable, and not only that, in a coaxial cable, if you have a malicious host, I mean not malicious may not be malicious. Suppose its card has gone

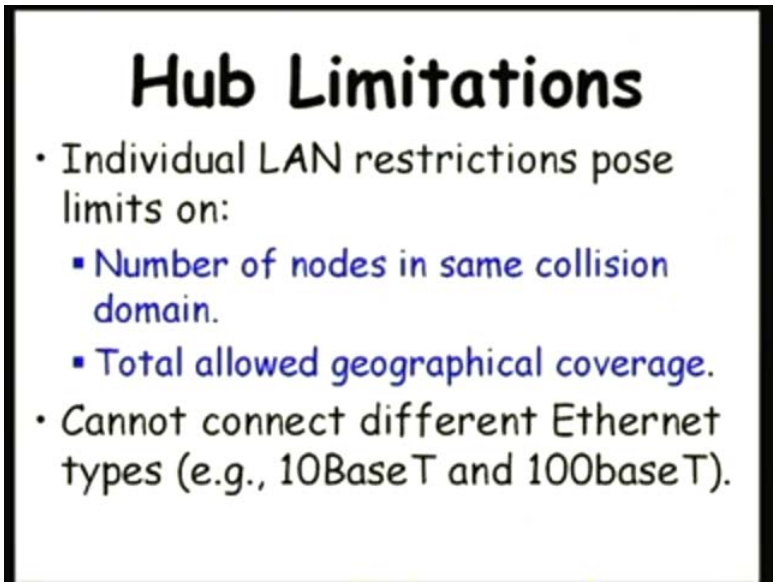
bad right, the LAN card has gone bad, it is just out putting noise or some junk signal on to the cable. So, that will make this fail. A coax cable will fail if one LAN card malfunctions, keeps on transmitting junk on to the on to the boss, but in a hub situation, the hub detects which node is misbehaving, excessive collision from some hub it can disconnect it. So, that way it is also more robust compared to a coaxial cable.

(Refer Slide Time: 41:13)



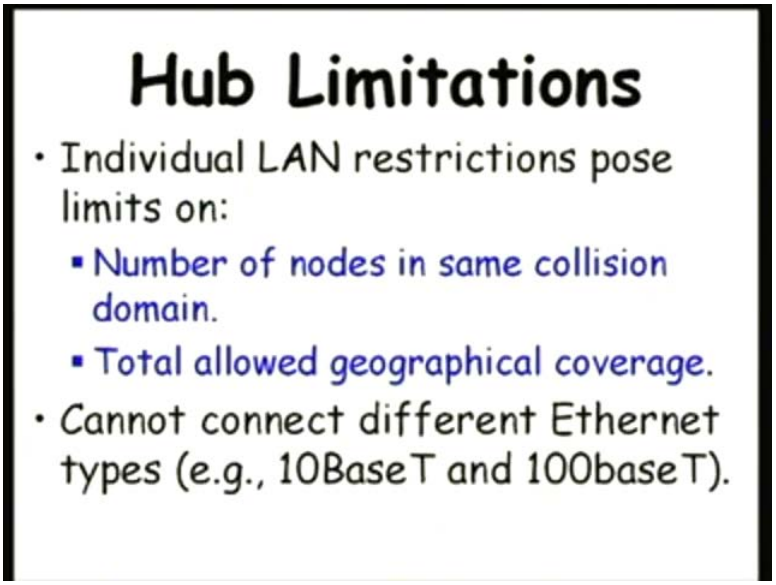
But again, the problem is single collision domain. Even if you have several hubs attached in a tree, there is no increase in throughput.

(Refer Slide Time: 41:25)



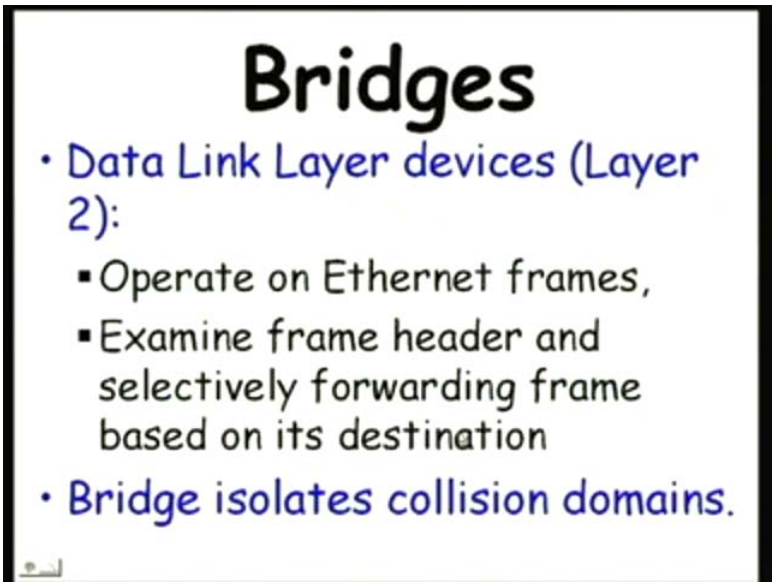
And multi-tier throughput is the same as a single segment throughput right. You agree with this, isn't it? Because the collision domain is the same. So, if it is a 10Mbps LAN, then even if you have a multi-tier arrangement, still the traffic supportable is 10Mbps right.

(Refer Slide Time: 41:55) ((No audio from 41:52 to 42:00))



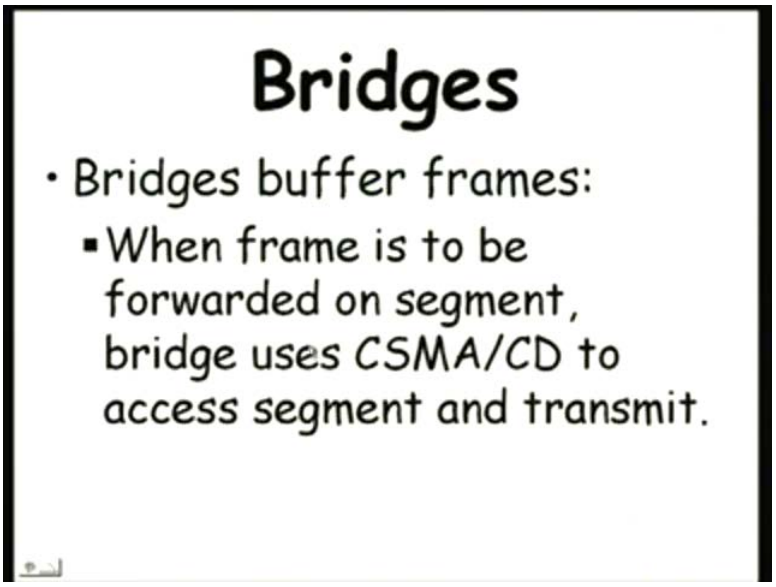
So, the geographical coverage is less and so on, and not only that, the hub cannot connect different types of LANs. For example, a hub cannot connect a 10 base T with a 100 base T because it is after all a repeater, isn't it. Whatever it gets on one port, it will repeat on the other port. So, if it gets a 100 base T bit, it will repeat here also for this the other segment and this will make no sense for a 10 base T. So, these are some of the limitation on hub.

(Refer Slide Time: 42:33)



And then we had the bridges. Layer two device unlike the hubs which were physical layer devices, just bit level they operated, but here they can examine the header, the physical address and selectively forward frames and they can important thing is they could isolate the collision domains because based on the physical address, they can either transmit or not transmit, either repeat or not repeat.

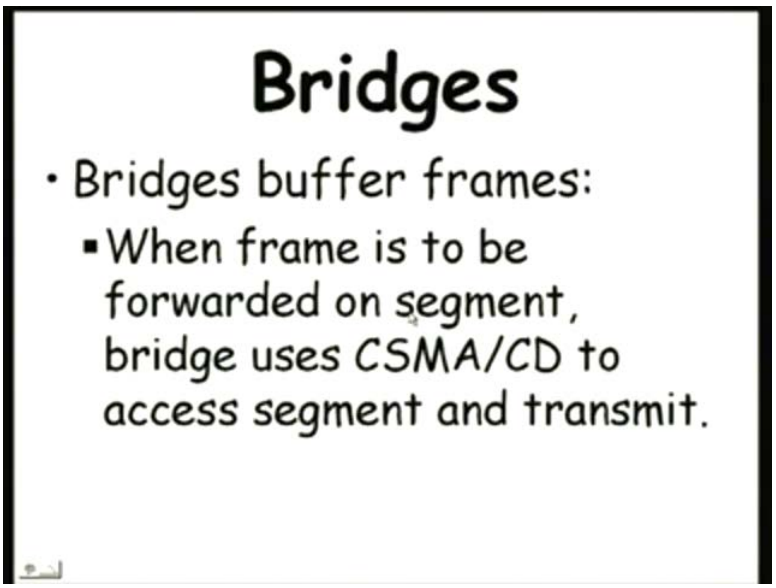
(Refer Slide Time: 43:09)



And not only that, their buffered frames… I do not know whether you have seen a bridge or no. Have you seen a bridge? How does that appear?

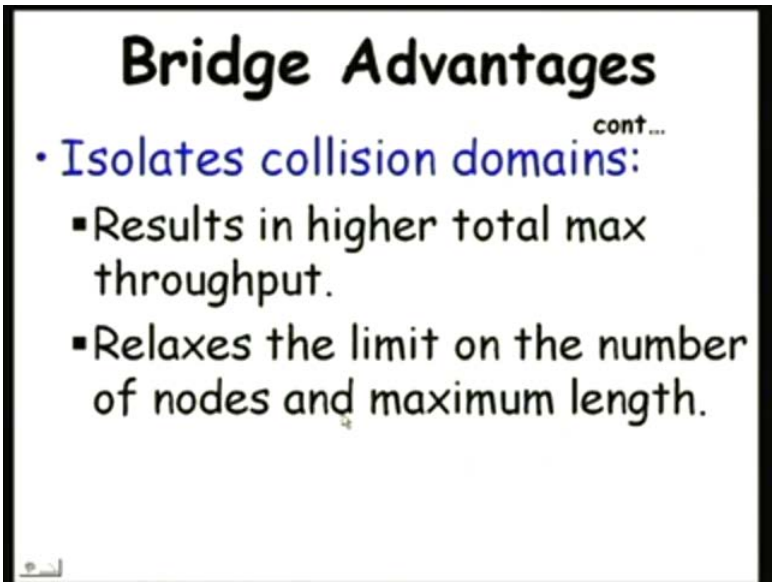
(Refer Slide Time: 43:28) ((No audio from 43:23 to 43:28))

(Refer Slide Time: 43:32)



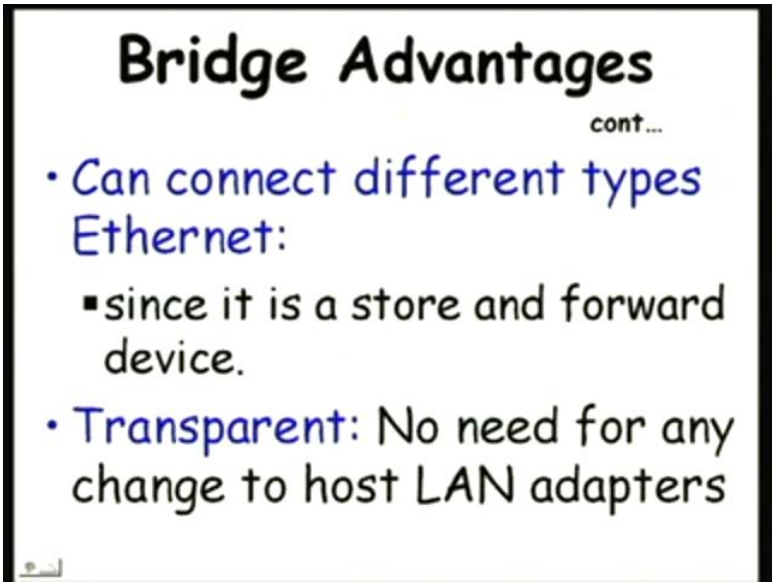
Typically they are implemented using a computer because they need to do several things like buffering frames and so on, typically implemented in software.

(Refer Slide Time: 43:45)



Isolates collision domains, higher throughput, relaxes limit on the number of nodes and maximum length, can connect different types of ethernet because it stores it, buffers them.

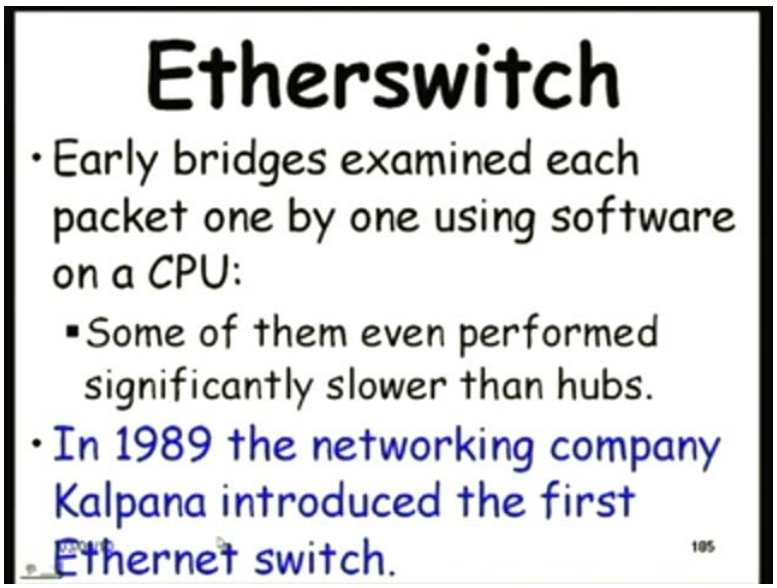
(Refer Slide Time: 43:57)



So, even it does not just transmit, once a bit comes need not just read out the bit without waiting for the next bit. Here it buffers them and a 10Mbps signal, a 10Mbps LAN, it can read out at 100 Mbps or 100 Mbps it can transmit on one port where a 10 Mpbs ethernet is attached.

So, it can inter connect different types of LANs. It does not just repeat the bits. It buffers the data. It is a store and forward device. First stores and that is the reason why it can interconnect different types of networks. And also it is transparent; you do not have to change the LAN adapters. It works with the same LAN adapters. You do not know whether you have attached to a hub or a bridge.

(Refer Slide Time: 45:00)

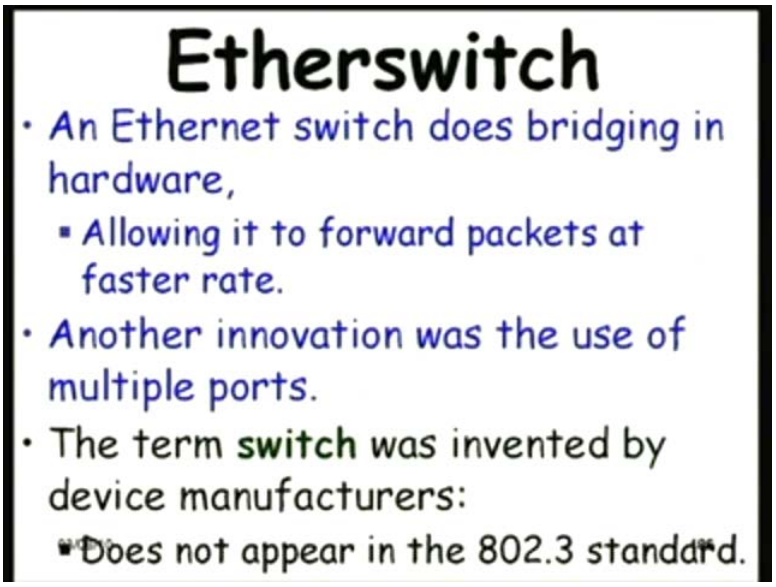


And the next development was a switch called as the ether switch; a development on the bridge. The bridge examined each packet one by one. As you were saying that had a CPU; many times looked like a traditional computer, a PC or something.

And it examined, it stored the packets, and there was a software, a software driven, examined each packet, and as a result because it was a software implementation, the bridge was a software implementation, it stored the packets, then transmitted. It performed even worse than the hubs.

In 1989, networking company; Kalpana networks; must be the many Indians in this company gave the name Kalpana networks, introduced the first switch, ether switch.

(Refer Slide Time: 46:08)

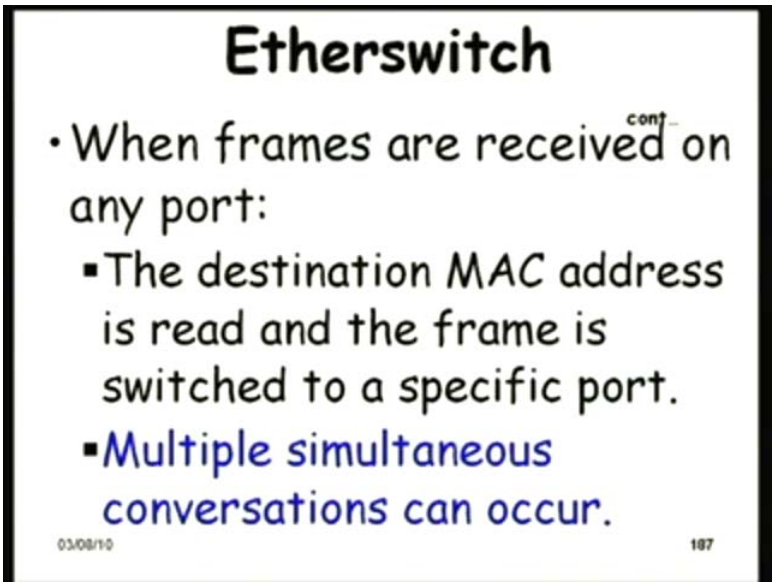


The idea was that there were several innovations actually. One is that it does bridging in hardware. It all these are implemented in hardware. The examination of the header and (( )) and forwarding. It could forward packets at a faster rate. Compared to a bridge which was a software implementation, the switch was a hardware implementation and also it used multiple ports. It could handle simultaneous connections at the same time.

In a bridge, at best, one connection can occur right, one can computer can talk to another computer, but here using the switch, there are multiple ports and each pair of the ports can talk to each other; multiple simultaneous interconnections can occur.

So, there are several innovations, and then the manufacturers are given the name switch. It did not appear in the standard. Later of course; become so popular the name had stuck people referred to the switch.

(Refer Slide Time: 47:25)

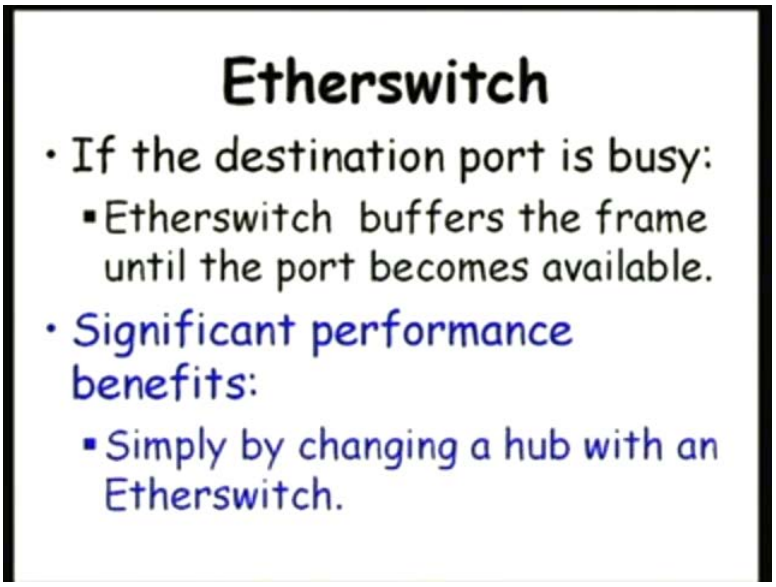


Improvement over the bridge and when the frames are received on any port, the MAC address or the physical address is read and the frame is switched to the specific port. This is also the bridge was doing this. It was doing it on software, here it checks between multiple ports. The connection, the data that is coming on different ports, checks on hardware the MAC addresses or the physical address, and then it switches the frame to the port where it is required.

And of course, how does it learn which desk, which address on which side that the port etcetera; the learning thing it is there in the bridge. We will not discuss about that, not spend time on that because it is not crucial to our further discussions. You can, those who do not know about that please read up networking book.

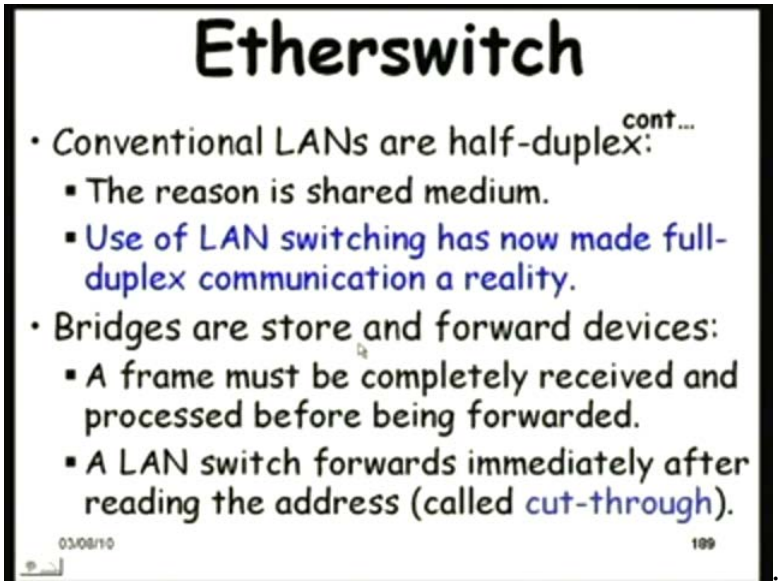
Multiple simultaneous conversations can occur, that is what we are saying. Compared to a bridge which supported only a single connection, here multiple conversation could occur, and there was a big improvement in the performance of a interconnection.

(Refer Slide Time: 48:43)



And not only that, it buffers the frame when the port becomes available, if the same port it wants a connection to a port which is already busy, it buffers the data. Significant performance benefits were noticed just by changing a hub or a bridge with a switch.

(Refer Slide Time: 49:08)

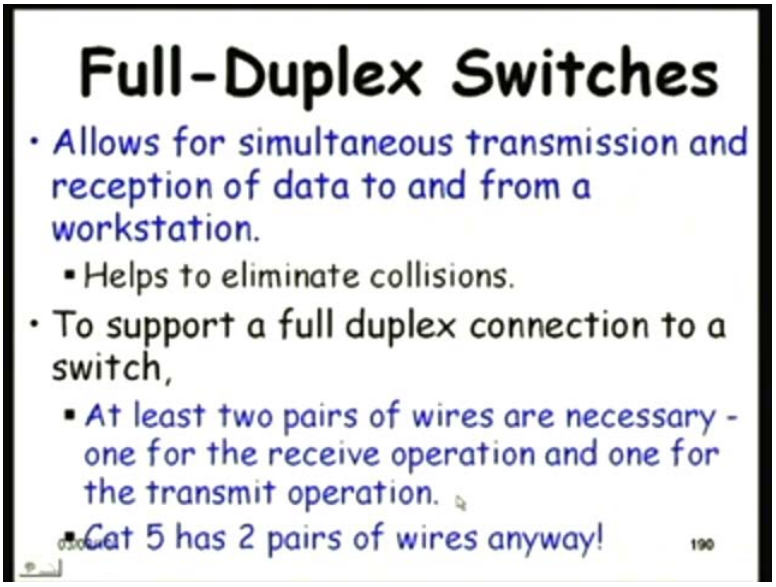


And also the full duplex communication became a reality. ((No audio from 49:16 to 49:20)) The same time, data can be received and also transmitted, and another improvement over the bridge is that it was a completely store and forward.

A frame is received, stored, header examined, and then transmitted. And there is a time involved, isn't. It receive the entire frame, examine and then start transmitting, but here its say cut through arrangement where, as soon as it finds the header, it starts forwarding called as the cut through.

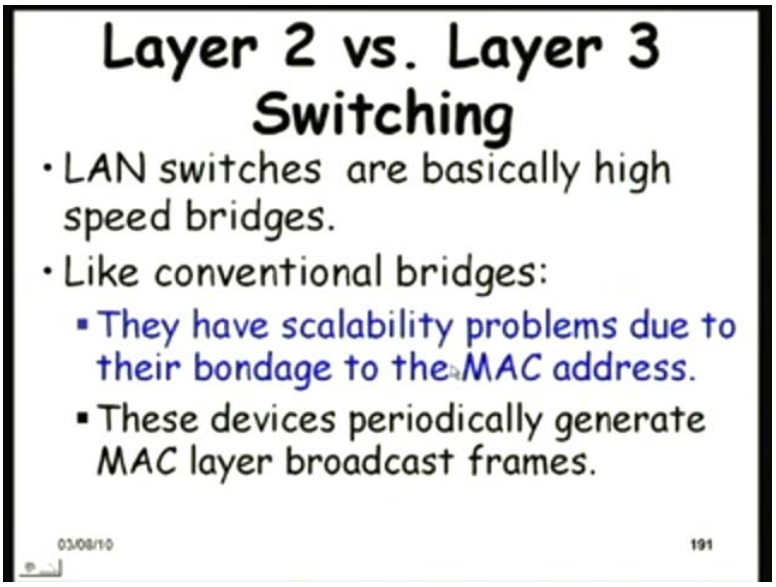
A switch forwards immediately after reading the address, but of course, there is a problem with this. The problem is that it would also forward corrupted packets, corrupted frames, because to check whether it is corrupted need to store it fully, isn't it. So, cut through has a problem which was later overcome. We will not discuss about that.

(Refer Slide Time: 50:25) ((No audio from 50:36 to 50:31))



It allows simultaneous transmission and reception data. It helps eliminate collisions because as long as they are connected to the switch, multiple simultaneous conversation can occur, and not only that, it is a full duplex switch, and naturally needed two pairs of wires to be connected, to transmit the receive and send signals, but cat 5 has two pairs of wires anyway. So, using cat 5 you can easily set up connected to a switch.

(Refer Slide Time: 51:17)



But might have might hear this term very frequently that somebody says we use a layer 2 switch and somebody says we use a layer 3 switch. The same switch right? What is this layer 2 and layer 3 switch? Anybody knows two types of switch? You will find in the market; layer 2 switches and layer 3 switches. What are those and what are I mean what difference does it make, whether it is a layer 2 switch or a layer 3 switch. Not very difficult to answer. So, the layer 2 switches are essentially high speed bridges, the layer 2 switches.

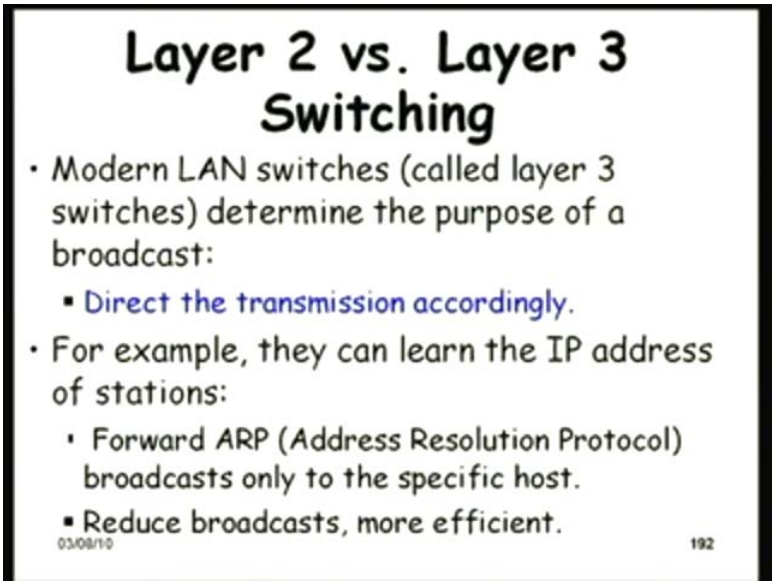
The bridges you know, they examine the MAC address or the physical address and the layer 2 switches are also operated in the layer 2 address which is the MAC or the physical address. And like the conventional bridges, the layer 2 switches have scalability problems because of their bondage to the MAC address, because you know the MAC address does not have much information in that.

If you know the MAC address of a host, you do not know, it can be anywhere in the network, isn't it. It does not have much information encoded accepting that 2 MAC addresses are unique, it encodes no other information.

But if it is a IP address, it also indicates where it will be located, and you can reduce the… you can direct it to appropriate place. You do not have to do a MAC broadcast to find out where it is located, right. So, that is the main advantage here.

The layer 2 switches periodically generate MAC layer broadcasts. Whenever they do not know, they have not learnt the port to which a host is attached, they will do a MAC layer broadcast to find out where it is, and very frequently they do the MAC layer broadcast and result in a high network load.

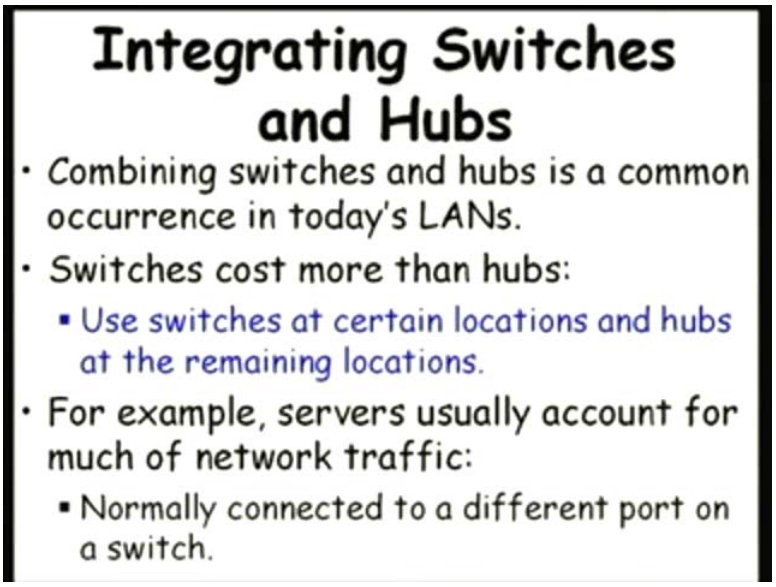
(Refer Slide Time: 53:35)



You can find layer 3 switches now a days which direct the transmission depending on what they interpret where the transmitter sorry the receiver, where it is likely to be located, they will transmit it on that port. Even they do not know that it is where it is, but just by examining the destination the IP address, they will know which port it is located and they will restrict the broadcast to that port only.

So, based on the IP address, they do the ARP or the address resolution protocol where they broadcast and find out which is the host. They do the ARP broadcast only on the specific port rather than doing a full broadcast on the network. And layer 3 switching naturally is more efficient.

(Refer Slide Time: 54:45) ((No audio from 54:36 to 54:44))



Combining the switches and hubs is a common occurrence in today's LANs. You go to our lab or anywhere, you will find that there are hubs as well as there are switches. So, which one do you connect where. Can you directly connect some devices to the switch; some computers and some to the hub say design decision actually. We will just spend a minute or two in the next discussion because again this is important as for our later discussion are concerned about the hubs and switches, and how interconnect the design decision of this.

So, we will just stop here today. We will continue from this point, spend few minutes on integrating switches and hubs, and we will continue from this point onwards. Thank you.