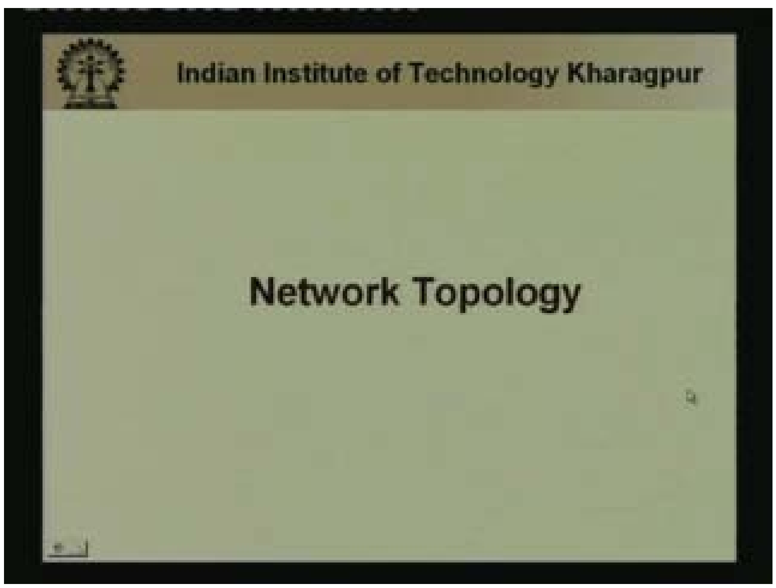
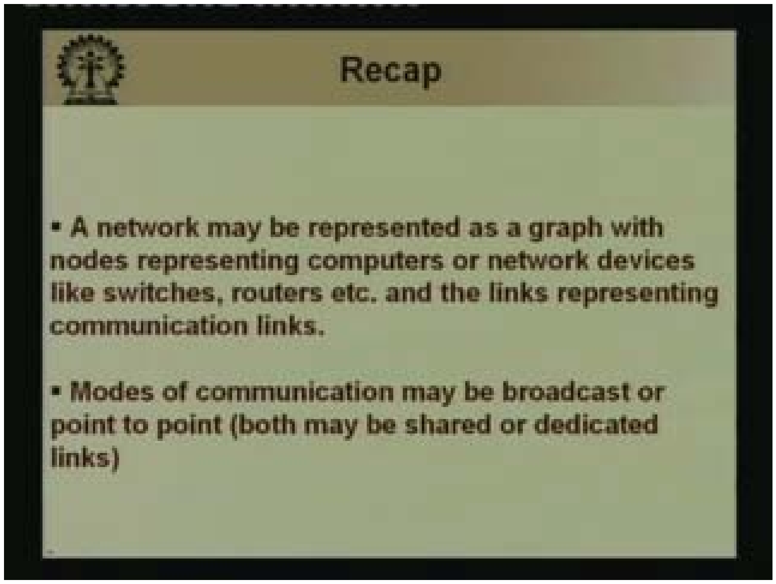
**Computer Networks**
**Prof: Sujoy Ghosh**
**Department of Computer Science & Engineering**
**Indian Institute of Technology, Kharagpur**
**Lecture - 2**
**Network topology**

Good day. In this lecture we will discuss the network topology. What do you mean by a network topology? We can just have a quick recap of what we have learnt last time. Basically a computer network could be a number of nodes, which are connected by some communication links. There is some kind of what we usually call a graph representing the network.

(Refer Slide Time: 00:53)



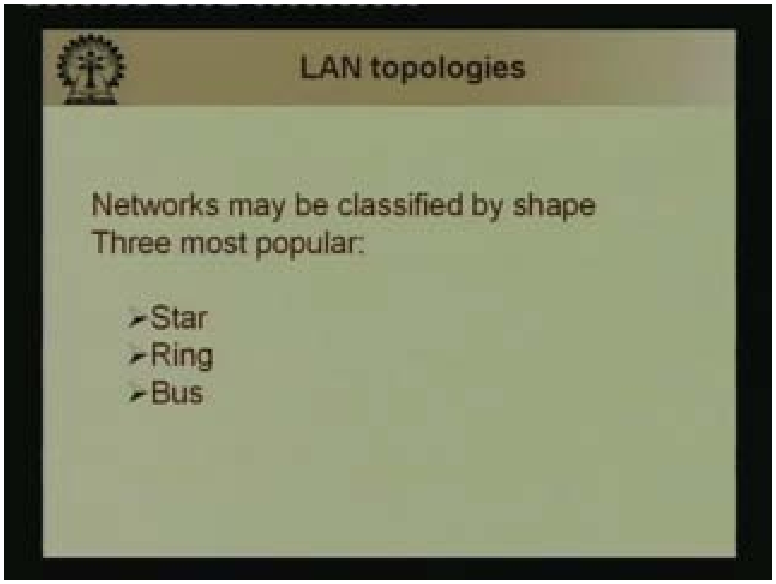
(Refer Slide Time: 01:15)




We can just have a quick recap of what we have learnt last time. Basically a computer network could be a number of nodes, which are connected by some communication links. There is some kind of what we usually call a graph representing the network. This graph has a certain structure. We talk about the structure. This structure has an implication about how will we communicate. I said it is in general not feasible to have one-to-one communication between each pair of node.

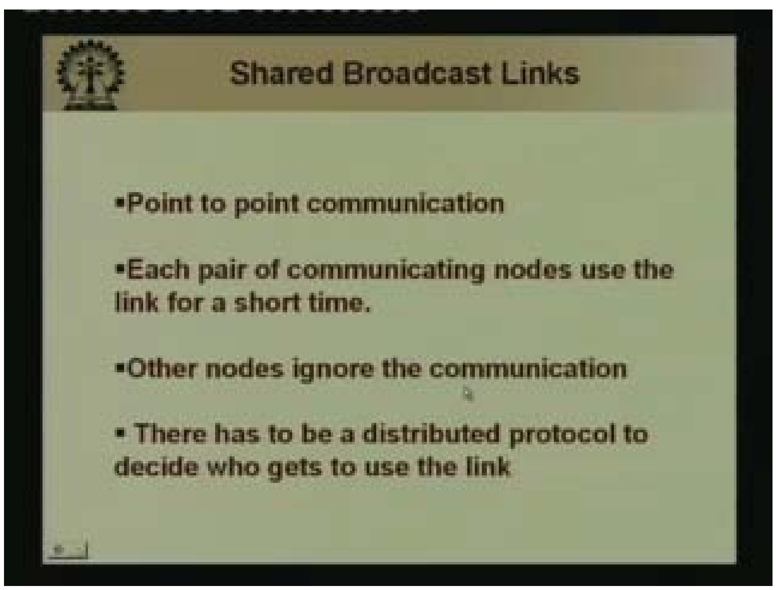
That is not possible at all. So, we need a structure formed by the nodes connected in some manner. That is the subject matter of discussion today. So a network may be represented as a graph. Nodes may represent computer or network devices like switches, routers, etc. and the links represent communication links. Modes of communication may be broadcast or point to point.

(Refer Slide Time: 02:34)




First let us talk about the LAN topologies. LAN is the local area network and local area network topologies are: star, ring and bus. We will just look at all of them.

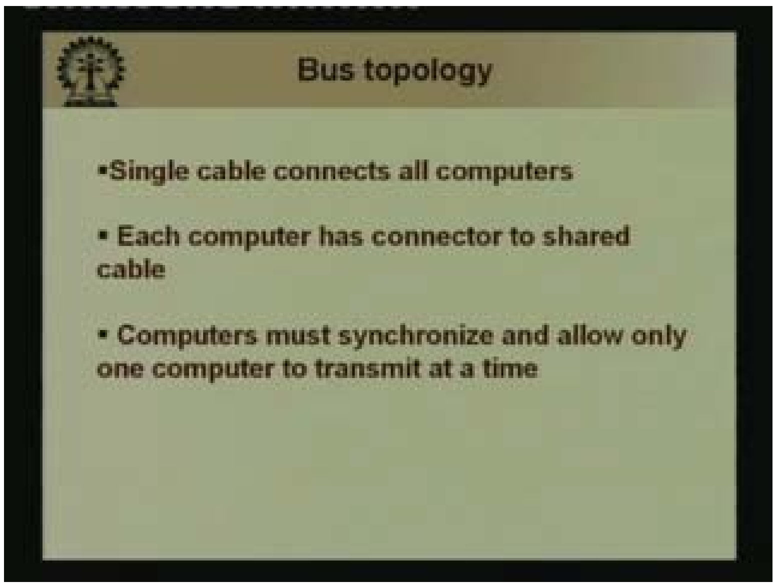
(Refer Slide Time: 02:59)




We first take up this bus topology as this is a very simple kind of network. This is based on a shared broadcast link. We want to have point-to-point communication. There may be so many nodes A, B, C, D etc., which are connected to the network. A wants to communicate to B; A specifically wants to communicate to B. So each pair of communicating nodes uses the link for the short time.

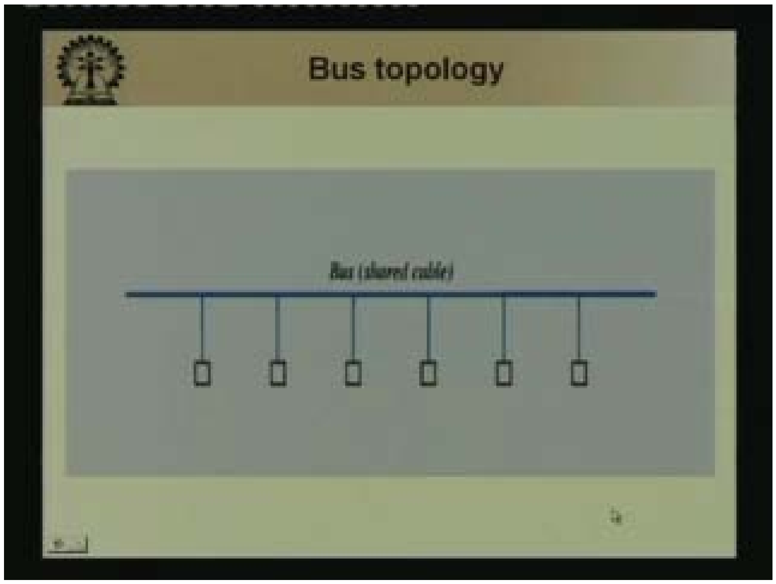
So A uses the link for the short time to send his message to B. After that is over may be C might send something to D or something like that. So other nodes ignore the communication. Since this is shared broadcast link, all the links are shared by all the nodes for the communication. Hence that is not private in that sense. So all the nodes get that communication but they usually ignore this communication whereas B will copy this for its own purpose. There has to be a distributed protocol to decide who gets to use the link; otherwise, communications will collide in that shared broadcast medium. The communication of both the pairs of node will get garbled. But we want A, B and C, D to get clear signal so there has to be some Distributed protocol to decide who gets to use the link.

(Refer Slide Time: 05:12)



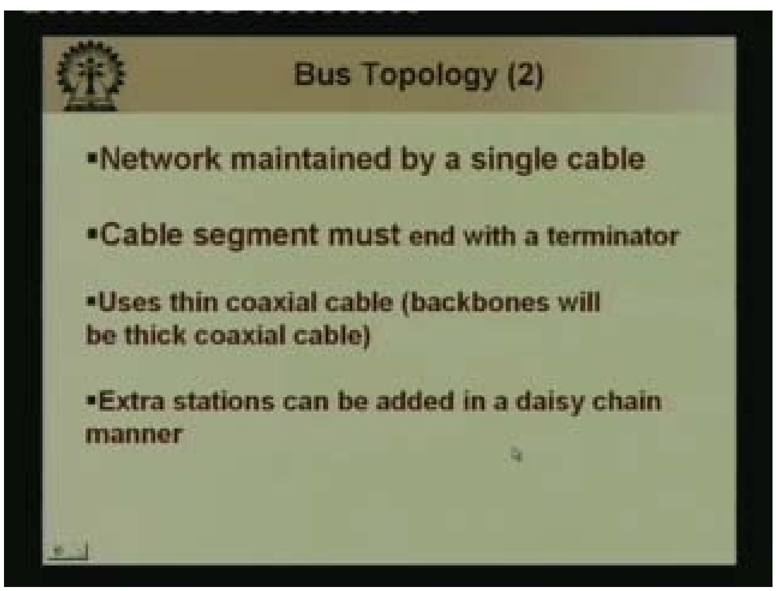

Now Let us see bus topology. What do we require? The simplest thing is a single cable. A single cable connects all the computers. It is as if the computers are hanging from the single cable. Each computer is connected to this shared cable. So computers must synchronize and allow only one computer to transmit at a time as per a protocol. But as such, the network is very simple network with a single copper cable So this is the picture of a bus.

(Refer Slide Time: 06:00)




We have this shared cable and computers are somehow connected to this. So A will communicate to B. B will simply broadcast over this medium. B will capture it. C, D, E, etc. Will all ignore this?

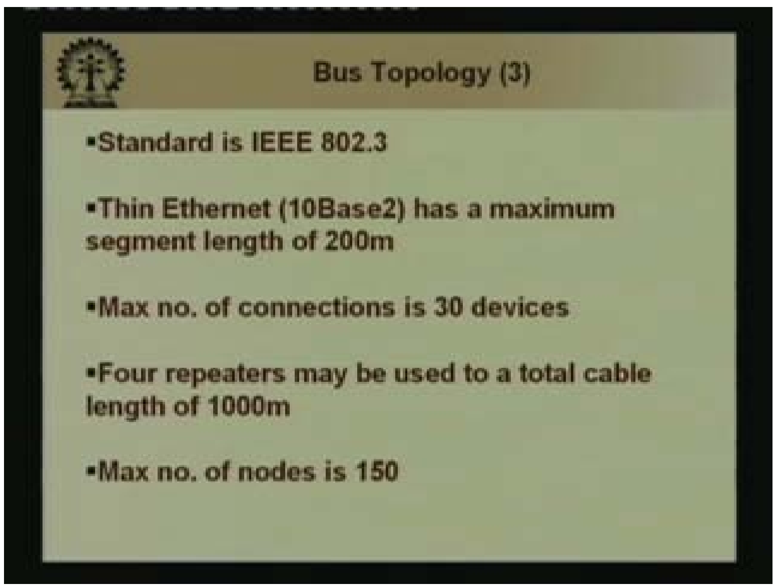
(Refer Slide Time: 06:27)




The Network is maintained by the single cable. Cable segment must end with a terminator. Otherwise, what will happen is that when some node, let us say A sends a signal on the cable not only  C, D, etc. will  Get it but it will get reflected from that other end if it is not properly terminated.

So it becomes a Kind of unwanted noise in the medium which we do not want. So the coaxial cable is used. There are two types of coaxial cables traditionally used. One is a thin coaxial cable called thin LAN and the thick coaxial cable called thick LAN and extra stations can be added in a daisy chain manner. This technology is sort of getting outdated at the moment. You still have maybe some thin and thick LANs here and there but mostly people are moving out of this and the main reason why the people are moving out of this is because this connection is likely to become loose and as soon as you have a loose connection you will have a problem in communication. There are some other reasons also why this technology has become Obsolete these days. But still if you have shared medium, I mean the technology of using a single cable with a single broadcast medium and some machines are sharing. So this something likes a bus topology.

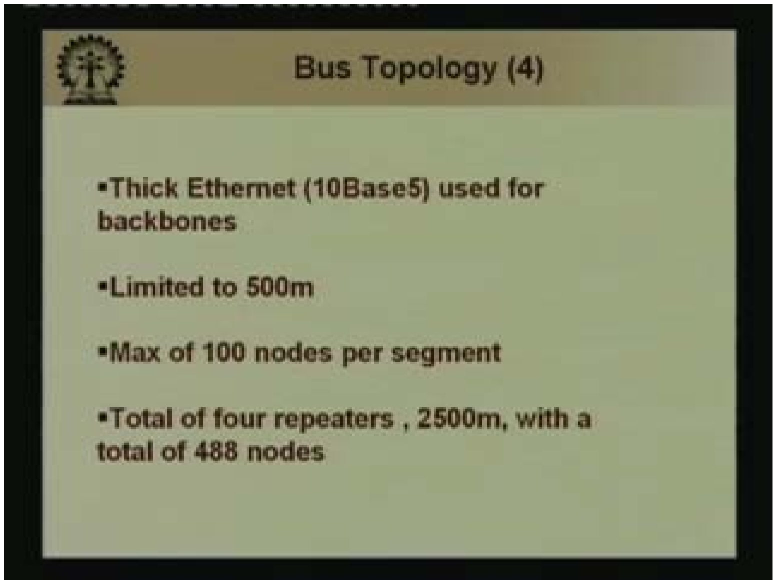
(Refer Slide Time: 08:26)




The standard which is used on this bus topology is IEEE 802.3. Actually what we do is to eliminate that cable and replace with something else. We will discuss that later. Thin Ethernet is the name of the technology when we use thin coaxial cable – we call it 10Base2. In this 10 stands for that it has a 10 Mbps speed whereas 2 stands for the maximum range of segment length of 200 meters. The maximum number of connections is about 30 devices.

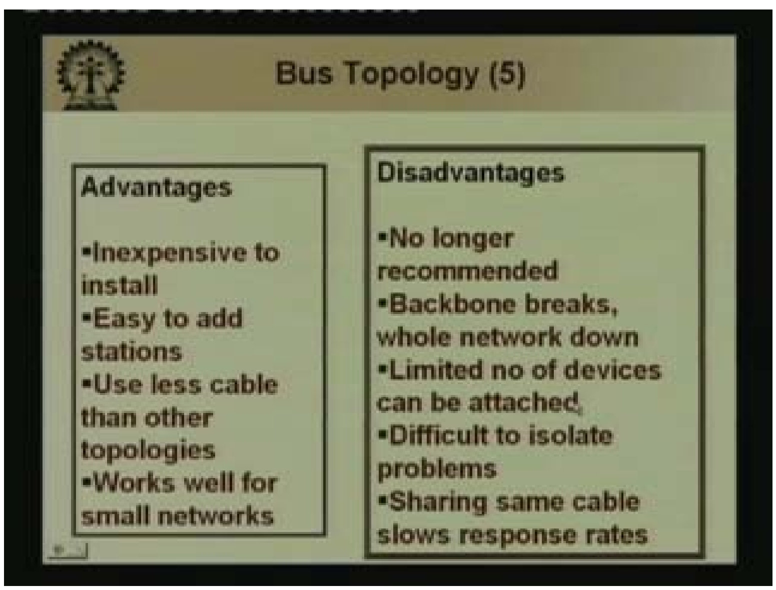
Four repeaters may be used to a total cable length of 1000 meters. If you want to have a very long cable, what will happen is that, as the signal travels down the line, the signal will get weak and as the signal gets weak you have to regenerate the signal and one way to regenerate the signal is to use a repeater over there. The repeater will simply take the incoming weak signal, amplify it and send the stronger signal down the line. The maximum number of nodes that you can handle here is about 150. Thick Ethernet, Which is the other version where you use a thick coaxial cable called 10Base5, also has the same speed of 10 megabits per second but length up to 500 meters.

(Refer Slide Time: 10:24)




So they were used for backbones that are limited to 500 meters with a maximum of 100 nodes per segment. That is somewhat more than a thin net and a total of four repeaters of 2500 meters. That is also somewhat more than thin net.

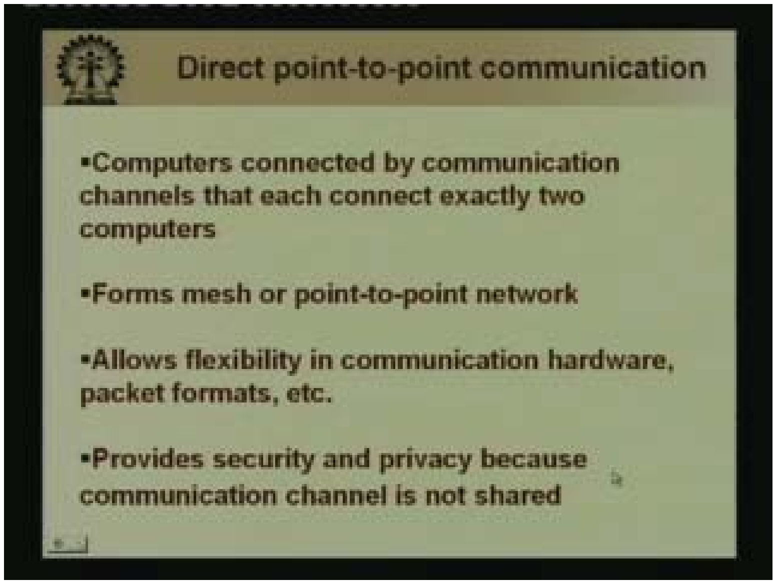
(Refer Slide Time: 11:05)




Now the bus topology has both advantages and disadvantages. It is very inexpensive as you have a simple cable. It is easy to add stations. You can have another punch on this cable and add new station that means a new computer. The amount of cable it uses is also much less and may be, it works well for very small networks. It is of course no longer recommended which means you will not get these parts any longer.

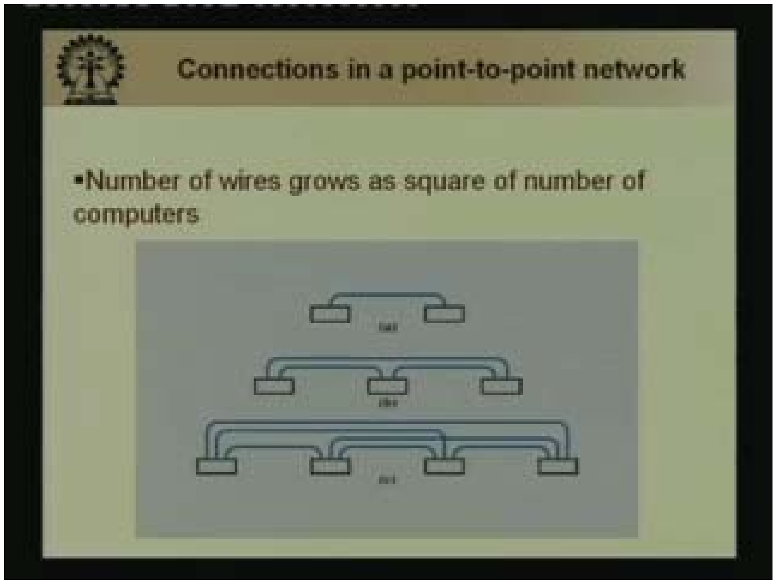
It is getting out of fashion because it is unreliable. This is much less reliable than the technology that we have today. The other disadvantage is that the limited number of devices that can be attached. It is difficult to isolate the problems. If there is a problem, then the whole network is down. Sharing the same cable slows the response rates now we come to direct point-to-point communication.

(Refer Slide Time: 12:43)




That means this is not shared. So this is some kind of a dedicated point-to-point communication. So computers are connected by communication channels that each connects exactly two computers. They are dedicated for this pair. So this forms either a mesh or a point-to-point communication, and thus a complete graph. We will come to that later. This is some point-to-point network. That means there is a dedicated link between some pairs of nodes. It allows flexibility in communication, hardware, and packet formats and also provides security and privacy because communication channels are not shared with point-to-point network, the network will look somewhat like this. We have these two nodes or three nodes may be connected like this.

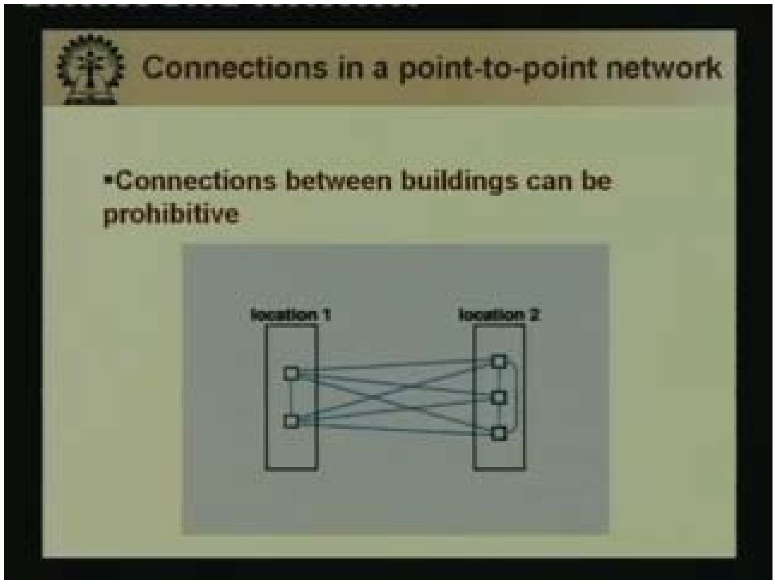
(Refer Slide Time: 13:52)




If we have four nodes and we want to interconnect everybody then we require six such cables. As the number of nodes goes to N the number of cables you require is going to be NC2 which is N (N − 1) by 2 which is approximately equal to $N^2$ which means the number of cables and the total length of cables that is involved are really increasing. But the kind of cable which is usually used is not as expensive as the previous thin LAN or the thick LAN. At the same time the amount of cable that you require becomes very high.

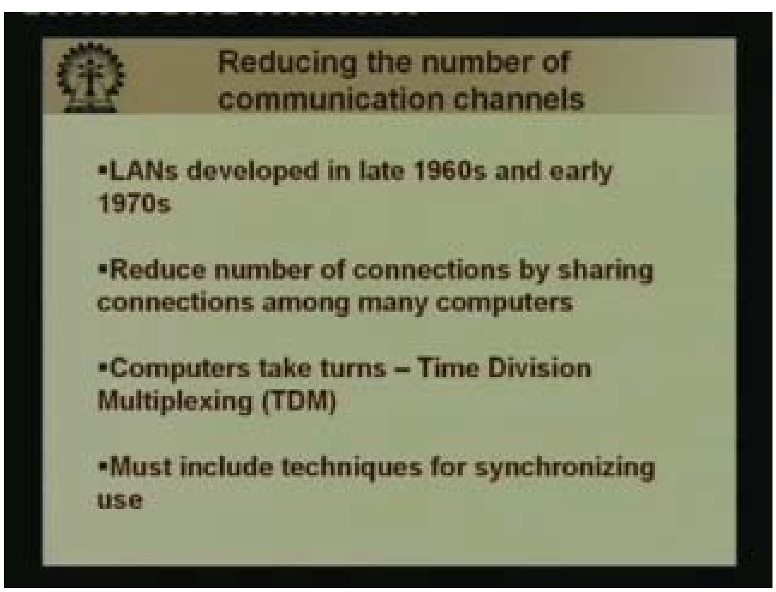
Hence this kind of structure is not really recommended for a local area network. Suppose you have, say, 10 nodes in a network and you are connecting everything to everything. That means every node to every other node and length of the cable for some reason, let us say, is not an issue. But then each node will be connected to 9 other nodes. This means that in this particular computer you will require 9 ports to which these cables will be connected. But that is not so easy to provide and this is another reason why, in a local area network, this kind of mesh topology is not recommended. We have an alternative for that.

(Refer Slide Time: 15:55)



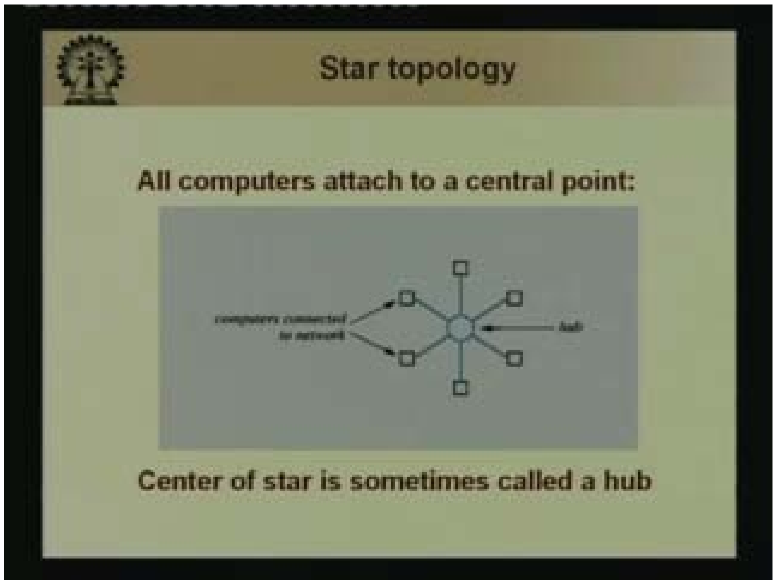

We are coming to that alternative. Another reason why you cannot connect everybody to everybody else can be illustrated thus: suppose there are two different buildings. Now the length of the cable will really become enormous because if you have N cables on one side and M cables, N nodes on one side and M nodes on the other side, you have a total of M into N number of cables which are running between two different buildings. It is lot of cables really. So if we want to reduce the number of communication channels we have to basically give up the idea of communicating directly in a LAN. It means that necessarily we share the connections among many computers. There are ways of doing this by multiplexing.

(Refer Slide Time: 16:34)



Here the computer takes turns in a very orderly fashion. That is called time division multiplexing and it also must include some technique for synchronizing the use. That means whoever wants to use that shared channel has to wait for his turn We Now come to this other topology, which is very common these days.

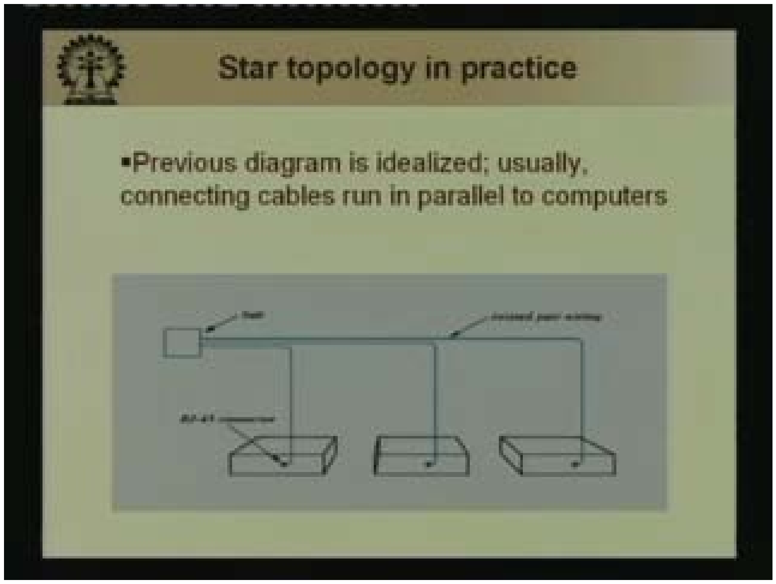
(Refer Slide Time: 16:34)




It is star topology. A star topology looks like this. There is a central hub (the centre of the wheel is called a hub) and a number of nodes are connected to this hub. I may at this stage mention that there is a physical topology and a logical topology. This is a star topology because it looks like a star. Its physical topology is that it looks like a star. Sometimes the hub is made in such a way that still this is a shared medium. What is the advantage of converting to what was previously a bus? It has some practical utility in the sense that (although the length of the cable is more in this case) the cable is a different kind of cable.

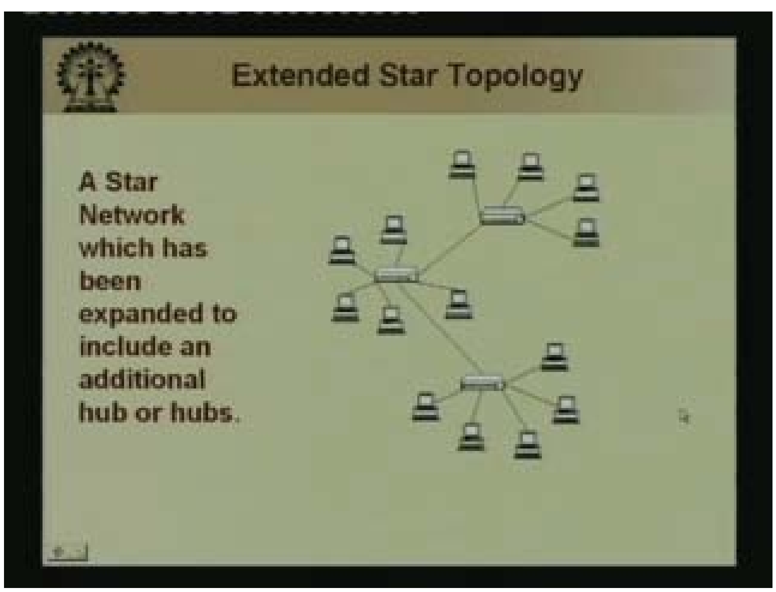
The cable connections are much better. They do not get disconnected very often. Furthermore when you bring all the connections together centrally, you can handle the connections at one central point. Whereas, if you have a long running cable, it will be difficult to locate loose connections. We will have to find out failures by going around so that becomes a bit difficult. So the physical star topology still maintains a logical bus topology, which is an important thing. Otherwise this hub or the central node may not be a shared medium at all. This is often the case these days Of course the previous star diagram is idealized.

(Refer Slide Time: 19:49)



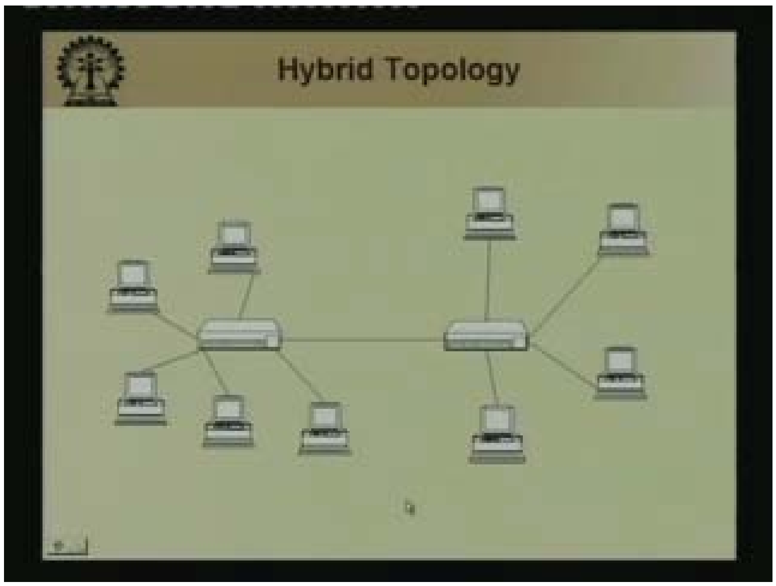

Usually you will have something like this. You have this hub somewhere and then you have these different computers connected and there is a number which is written over here: RJ-45 connector which is the kind of connection which has become almost ubiquitous. These cables are something like the kind of cables which connect your telephones. They are called UTP cables or unshielded twisted pair cables. They are basically easier to handle and are also cheaper. These connections go on to the RJ-45 connectors on both sides. They are much more reliable than the previous thin LAN or thick LAN but the physical diagram may look something like this.

(Refer Slide Time: 20:50)



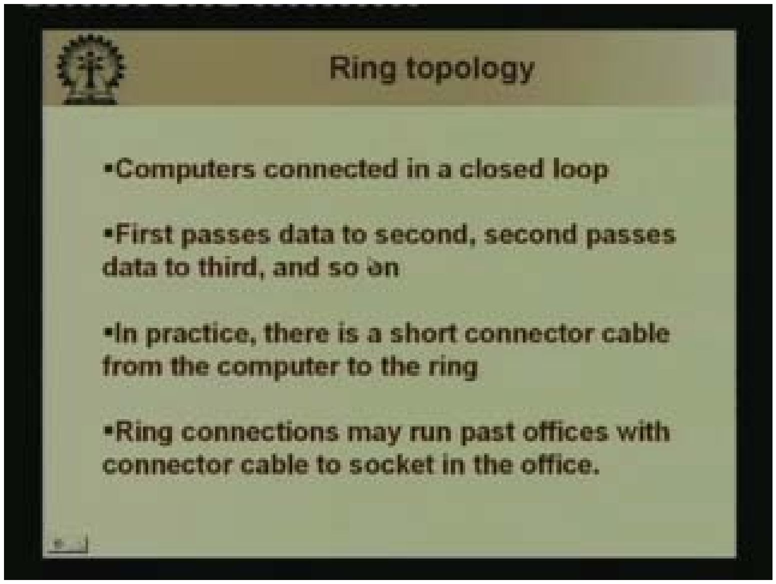
You can have an extended star topology, which means different stars may be there, which are connected in some manner. That means the hubs in those stars are connected and those hubs may be shared but may not be shared medium at all. They may be what are known as switches. These switches are connected. If you look at this diagram, you have these different switches and from each switch we have a star connection to the different computers and the switches are connected in some fashion. You can call this also as a star. This is called extended star topology you may have a hybrid topology.

(Refer Slide Time: 20:50)



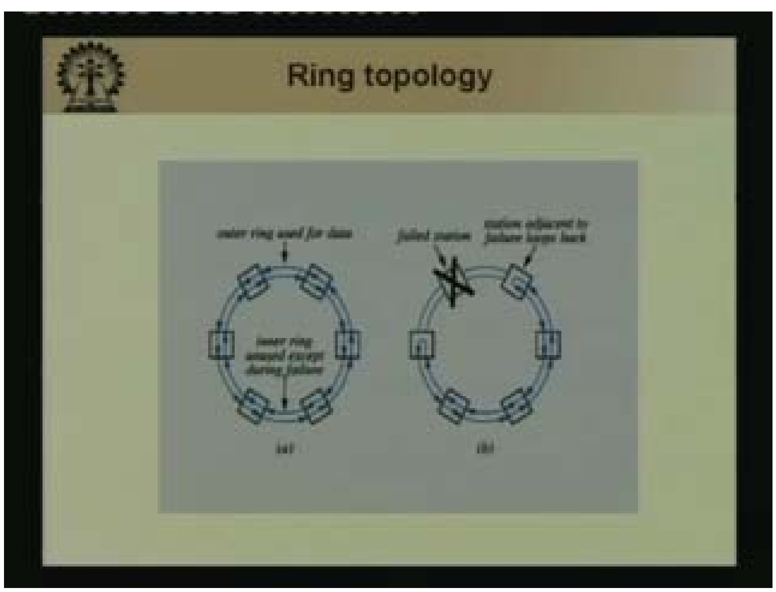

Some part of the network may be on a shared medium Some part, maybe, is not shared and even in some part, you could also have a coaxial cable running, leaving a thin LAN or thick LAN although that is becoming less common these days.

(Refer Slide Time: 22:04)




Now we come to another topology, which is also very important topology, called as ring topology. In ring topology, computers are connected in a closed loop. This has a lot of advantage. The way it works is that the first node passes the data to the second node; the second one passes the data to the third and so on. The data will go on hopping around the ring and what will happen is that, as it reaches the destination, if it will go around in a loop, it will surely reach the destination at some point of time. The destination will copy the same. In practice there is a short connected cable from the computer to the ring. Ring connections may run past offices with connector cables to sockets in the offices.

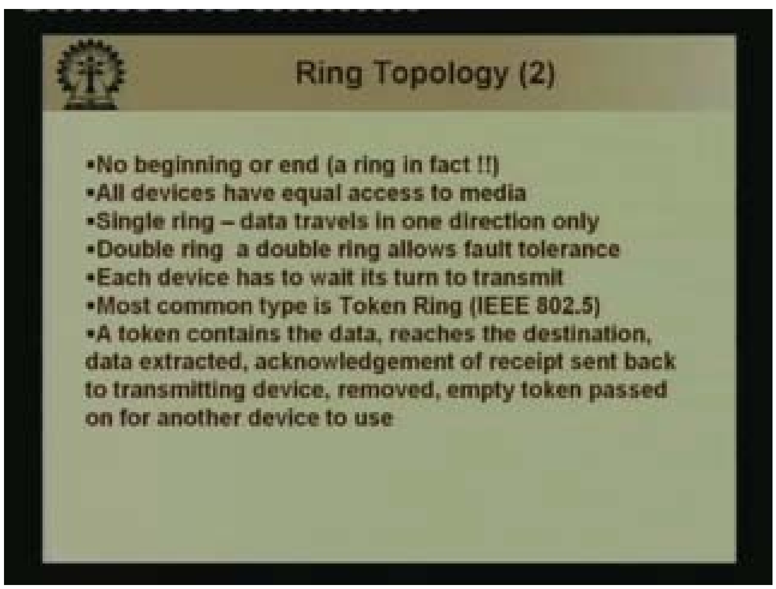
(Refer Slide Time: 23:04)



This is an example of a ring topology. Actually, there are two rings. In a ring the data will always go in only one direction. If your destination is on the wrong side then the data has to come over the whole loop and then reach the destination. So there is one ring for that. What is the other ring for? We put two rings or sometimes may be even three or four (two is quite common). One important reason for putting two rings is that if there is a failure in the network there is a possibility of the communication still going on. Look at the picture B. Let us say one particular node has come down. That means, there is some problem in this thing.

If these nodes can sense that this has really gone down, they will sort of wrap the ring around. Now physically this still looks like a broken ring. But if you look at it as a single ring, this is still a ring going through the nodes. These nodes can still communicate although there is a breakage over here. Either this node may break or this link may fail. So many things may happen. So this fault tolerance is one good reason for using rings. Especially in the wide area network, we have a lot of things. For example, let us say, these telephone exchanges are connected in some fashion using fiber optics cable. We will be talking about all those things later on. But they usually put them on a ring because if the cable is cut at some place they can still communicate by using the trick that I have just shown.

(Refer Slide Time: 25:46)




This is the summary of the characteristics of the ring topology. There is no beginning or end. It is actually a ring. All devices have equal access to media. One good thing about it is that all of them should get data at some particular point of time. So they have equal access to this media. In a single ring, data travels in one direction. Only a double ring allows fault tolerance. Each device has to wait its turn to transmit. That means you cannot start transmitting as soon as you want to transmit. You have to take your turn; and most common type is the token ring. Token ring has got its IEEE standard number (IEEE 802.5). In a token ring what happens is that the token contains the data.

It reaches the destination. Data is extracted, acknowledgement of receipt sent back to transmitting device, removed, empty token passed for another device to use. That is one way a ring can be used. For example, you make a data packet with this token as well as whatever you want to send to the final user. So this whole packet will go over to the next node in the ring this way, it keeps hopping from one node to another till the destination when the destination gets this packet, it knows that.

The destination had this or some kind of identification which will be there somehow in this whole bunch of data. The destination node will know that this is meant for it. It will extract the data. It may be put in an acknowledgement if you are using the protocol which uses acknowledgement and send it along the ring. It will go around the ring and come back to the original sender and the sender will know that this data has been received. That will remove this acknowledgement also and the empty token is passed and this token keeps on circulating in the ring. Whoever wants to transmit has to wait till it gets the token. As soon as it gets the empty token it will put in the data that it wants to send and send it along in the same way.

(Refer Slide Time: 28:25)

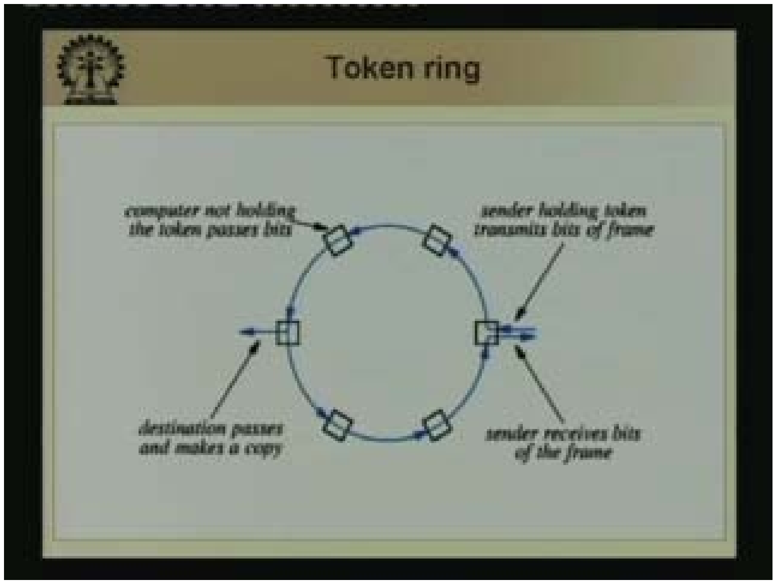

Ring topology has its advantages and disadvantages. The advantages are that, Data packets travel at great speed. Now one reason why data packets can travel at great speed is that this is a very synchronous operation. If you remember that in a shared medium where the nodes are not synchronizing their actions, what might happen is that two different nodes may start transmitting at the same time and then their data will collide in the broadcast medium, hence killing both the communications. Here such a thing cannot happen because it has all been synchronized with the help of the token. There are others ways of synchronization. We will come to all that later on. Data packets can travel at great speeds. There are no collisions. It is easier to find faults and rectify faults and terminators are not required as in an ordinary cable. The disadvantages are: it requires more cable than a bus and a couple of breakdowns may bring the entire ring down.

Smaller rings exist nowadays but anyway they are not very common. This is not as common as the bus so far as the local area network is concerned. In a wide area network a ring is very common. As a matter of fact the ring is the most common topology that wide area network could use.

(Refer Slide Time: 30:08)

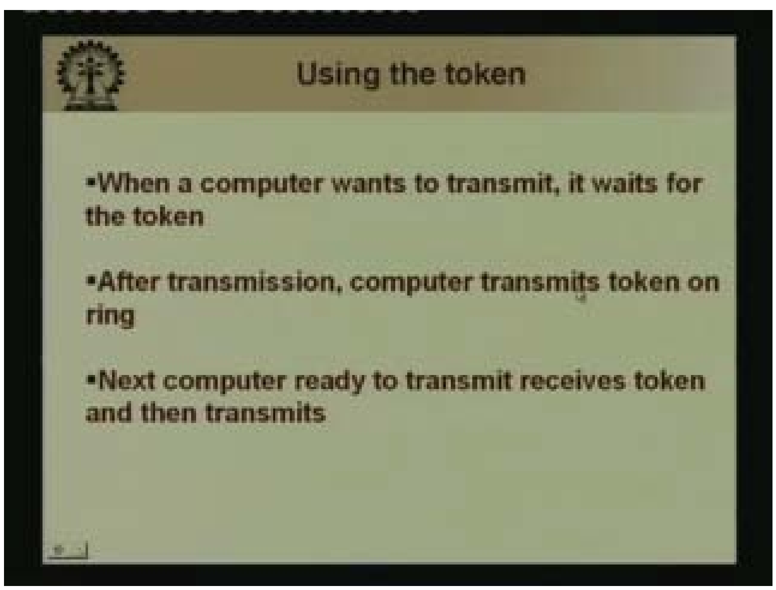

Many LAN technologies that use ring topology use token passing for synchronized access to the ring. The ring itself is treated as a single shared communication medium. Bits pass from transmitter past other computers, and are copied by destination. Hardware should be designed to pass token even if attached computer is out of commission. This is a small technicality. If the interface of the computer to the ring can function independently of the computer, that will be nice, because even if the computer is shut down, other people's communications are not affected.

(Refer Slide Time: 31:01)



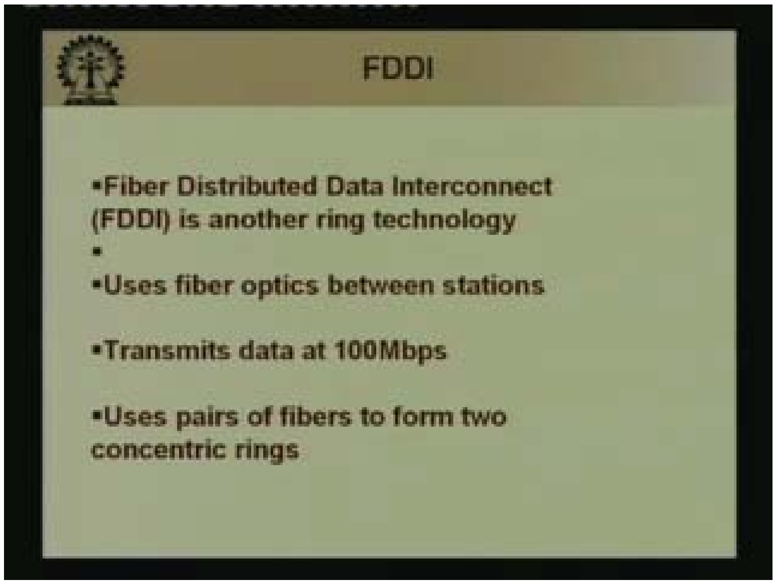

This is a picture of the token ring, in which the sender holding token transmits bits of frames. Computer not holding the token passes the bits as they go around, circulate at a very high speed. The destination passes the bits but it makes a copy and the sender receives the bits of a frame and it goes out. This is one way the network could work.

(Refer Slide Time: 31:39)




When a computer wants to transmit, it waits for the token after transmission. Computer transmits token on the ring to the next computer ready to transmit. It receives token and then transmits. This token ring was originally part of a LAN technology.

(Refer Slide Time: 31:54)

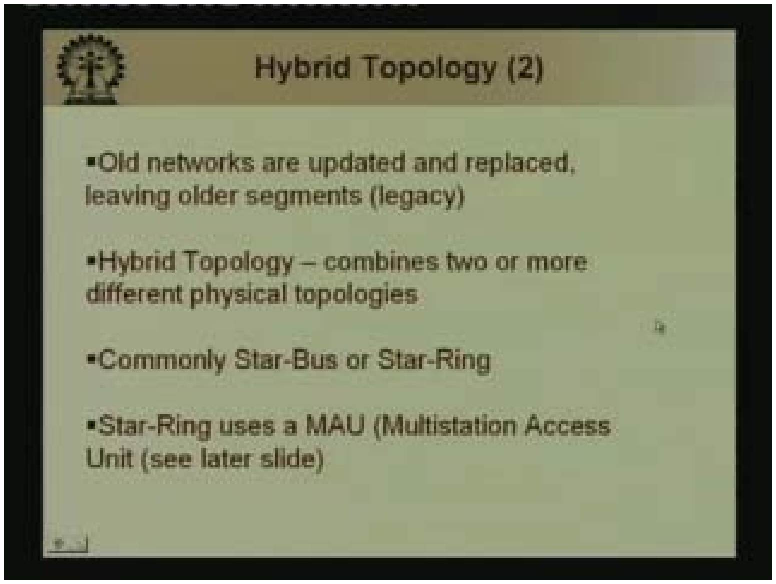



But then it fell into disuse. First of all the token ring devices were less common. They were more costly. Hence the token ring as a dominant LAN technology went out with time but one version of it called FDDI lived on and that lived on due to the very specific advantage that the ring topology has which is fault tolerance. This technology is called FDDI. In a FDDI, the ring is made of fiber optic cables. Multi mode fibers or even single mode fibers can be used. They use fiber optic cables in which we can send data at a fairly high speed. But the speed available is not comparable to the level possible.

Nowadays FDDI technology is also not that new. It is aging and that way its speed may sound less today. But when it was proposed it was taken as a very high speed. The basic reason why somebody still would like to use FDDI is its inherent fault tolerance capability. That is the technology, which is used in LAN, and it is fault tolerant.

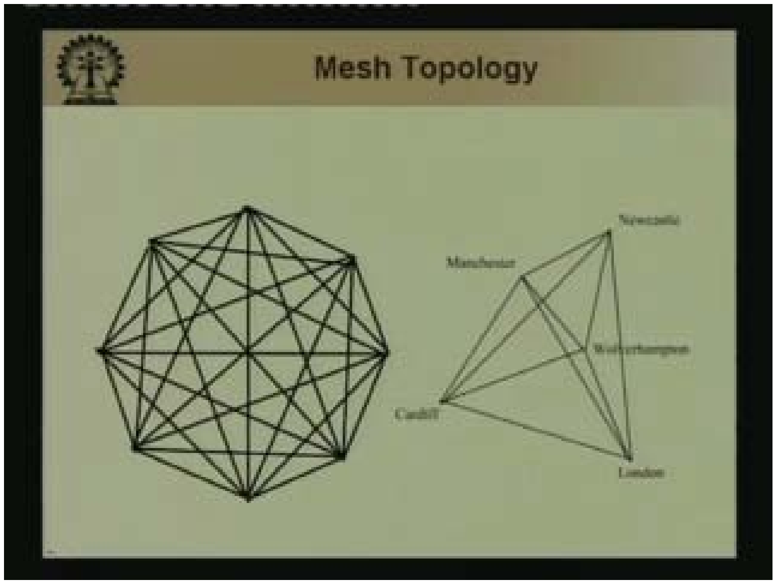
Ring technology, which is fault tolerant, is extensively used. Some other technology is extensively used in WAN but in the LAN we have this FDDI technology whose full form is fiber distributed data interconnects. This is another about ring technology which uses fiber optic between stations, which transmits data at 100 Mbps. When we were talking about the thin LAN and the thick LAN we were talking about 10 Mbps speed – 100 Mbps was an order of magnitude high when it was proposed. It uses pairs of fibers to form two concentric rings in order to get the fault tolerance we require with two fibers or two rings.

(Refer Slide Time: 34:23)




As soon as a fault occurs somewhere, the FDDI will automatically switch off and communication will not get disturbed. Furthermore you can have hybrid topology in the sense that you can have a ring, which emanates from the various nodes of the rings. Stars will form; they will be the different hubs of the different stars and these different hubs can be put in a ring. As a matter of fact, this is the very common way how FDDI is configured. Some FDDI switches form a ring and from each of these FDDI switches, we can start other kind of technologies like Ethernet etc., which form a tree-like structure. The other reason why you could have hybrid topology is that older networks are updated and replaced, leaving some older segments. You have replaced one part of network; you will get a hybrid kind of topology. Thus it combines two or different more different types of topologies. The common one is star bus or star ring. Starring uses an MAU (multi-station access unit), which is basically a part of FDDI.

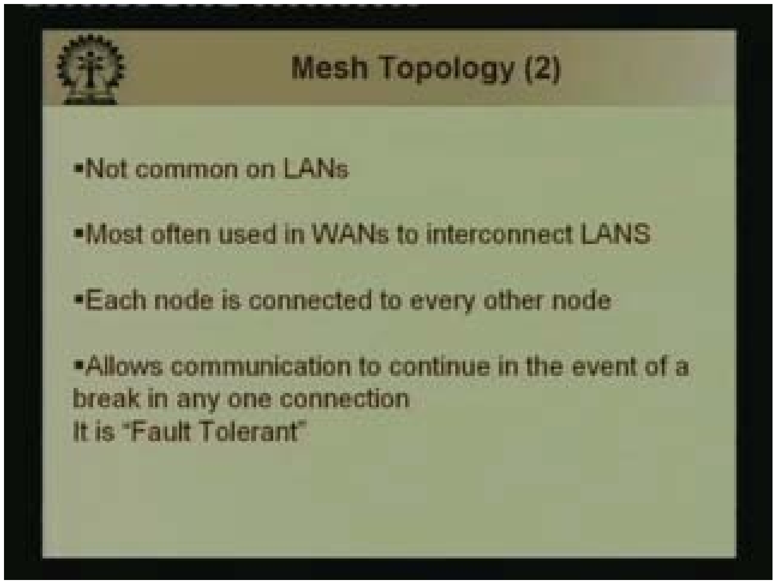
(Refer Slide Time: 35:54)




Next we take up the study of Mesh Topology. By a mesh or a full mesh, it is meant a complete graph as shown here. As discussed earlier, a complete mesh would take a lot of cable. But at the same time with complete mesh we have lot of alternative paths from any node to any other node. The diagram shows eight nodes and each one of them is connected to every other node now. Between any two nodes, you will have direct path and indirect paths as well. We have many paths for going from the same source to the same destination. This means that when one of the links breaks, all of them can still communicate without any problem. As this arrangement takes lot of cables, we do not use this. What we use is a partial mesh. In a partial mesh some of these links would be dropped, taking care that none of the nodes becomes disconnected. But all the links of the mesh need not be there even in the partial mesh.

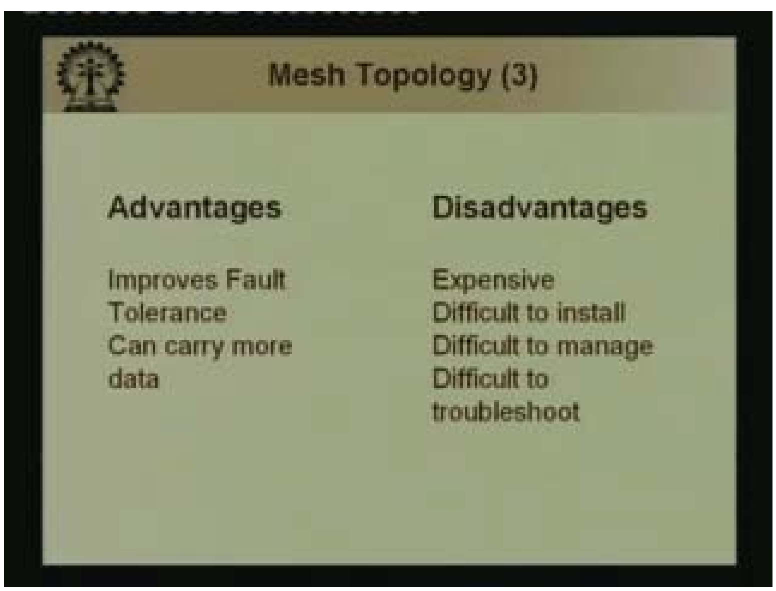
We can still have some form of redundancy and thus have some level of fault tolerance. But it may be not as much as one available in a full mesh. For Such a partial mesh the network topology is not well specified and it is difficult to evolve a protocol like token passing protocol. So here you have to have some other method of sensing the faults and correcting them. That becomes more complicated but the partial mesh topology is used in many places.

(Refer Slide Time: 38:49)



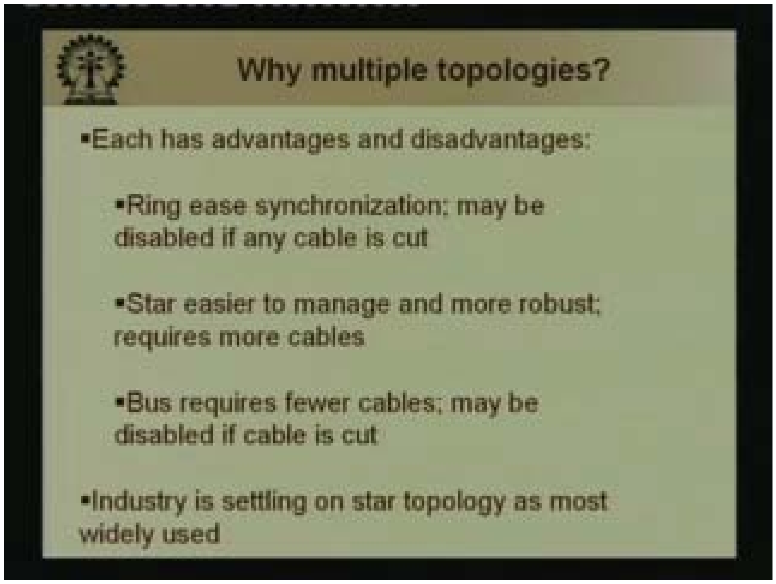

Mesh Topology of course is not common on LANs. These are most often used in WANs to interconnect LANs because WAN links usually are costly. The users of a WAN link naturally expect a certain grade of service. That is why the WAN service providers usually keep alternative paths. If one of the paths becomes unavailable due to some node failure or due to some link failure then it can still send the traffic across the WAN through some alternative paths.

(Refer Slide Time: 39:56)



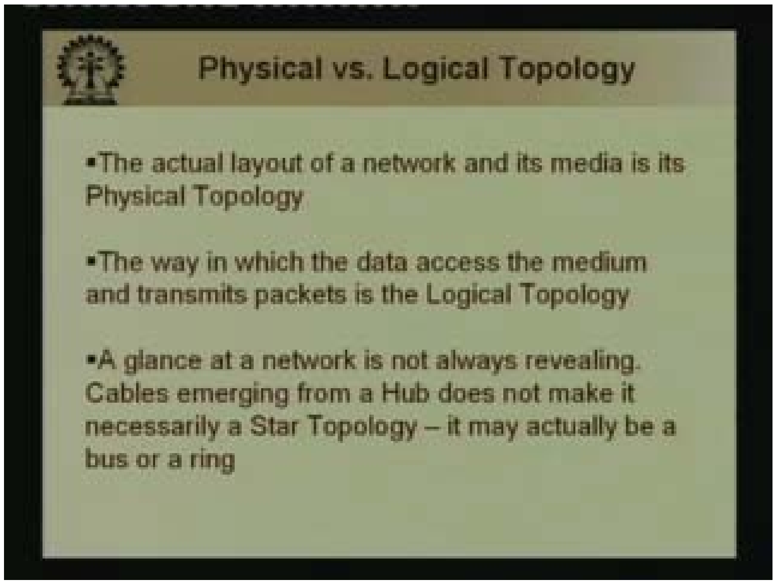
So the pros and cons of mesh topology are like this. The advantage is of course it improves fault tolerance and it can carry more data. The disadvantages of course are increased cost installation, difficulty in management and troubleshooting.

(Refer Slide Time: 40:41)




Now we have seen that each of these topologies has advantages as well as disadvantages. Rings ease synchronization, but it may be disabled if a cable breaks. Star is easier to manage and more robust but it requires more cable. Bus requires fewer cables, may be disabled if cable breaks and is not so reliable. Bus would not have fault tolerance really. So as far as the LAN is concerned, people are gravitating towards star topology. That means some nodes or some computers may be connected to a switch and then some other computers may be connected to some other switch and then these switches will get connected in some fashion. Extended star topology is the most common topology as this is emerging in local area networks. In wide area networks we have both rings as well as mesh topologies.

(Refer Slide Time: 41:21)

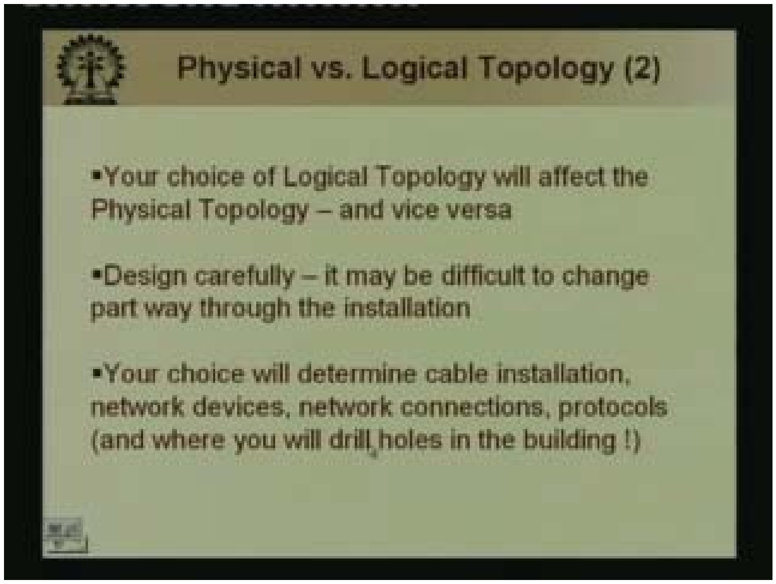



The physical and the logical topologies may be different. Something will look like a physical star but it may actually be a ring. Let us look at the following examples. Suppose you have this as the hub of the star and we have these three stations A, B, and C; we have say cable ducts running over there like this, through which a number of cables are passing. At the central hub you might connect two cables like this and then more pairs of cables in a similar manner.

Because this is one central place you can do this. What you essentially have is a ring. What you essentially have is a ring. Similarly, you can have any other kind of topology. Suppose you have a number of cables coming in like this. Now if we have a connection like this and similarly in all other places, then you can actually have a mesh. Although all this is within one physical duct and another physical duct going to nodes A, B, C, and D, it looks very much like a physical star but the actual connection is something like a mesh. Just as I could make a star, I could make it a mesh also. The media is the physical topology whereas the way in which data access the medium and transmits packets is the logical topology. A LAN at a network is not always revealing.

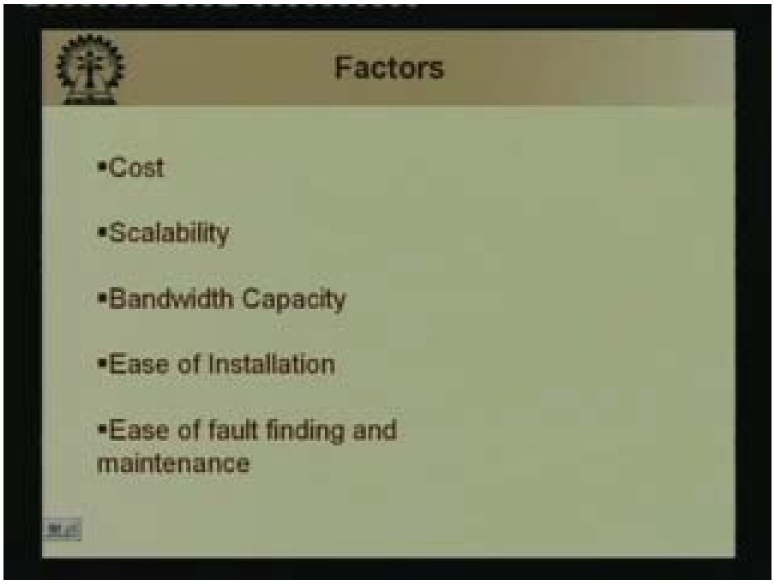
Cables emerging from a hub do not make it necessarily a star topology. It may actually be a bus or a ring. In a star topology, there is some piece of network box, which is called a hub. This hub actually replaces the single cable. This is again a shared medium. If they are connected like a star it has got the star connection. People use hubs these days but they do not use the single cable like thin LAN and thick LAN. Though it looks like a star, depending upon what kind of box it is, it could be actually a bus. Similarly as I have shown you, it could be a ring also.

(Refer Slide Time: 46:14)




Now the choice of logical topology is going to affect the physical topology and of course the other way around. The kind of physical topology you will have will also dictate the kind of logical topology that you can have. The kind of logical topology you can have will depend on two things – one the actual physical topology, the number of cables you have etc., another is the type of network boxes like switches, hubs or whatever you have as the nodes. We have to design carefully because it may be difficult to change the part way through the installation. When you think about designing a network, you have to put the physical topology min place to get the correct logical topology. Your choice will determine cable installation network, network connections and protocols and spots where you will drill holes in the building.

(Refer Slide Time: 47:33)




The different factors which you take into account while deciding on a particular topology are: the first thing that comes is what kind of technology you are going to use – there are different kinds of LAN technologies – for example, if you are using FDDI, then you have to have a logical ring somewhere. If you are using the Ethernet, you may have an extended star topology. The kind of technology you are using is a factor and of course this technology will have some cost benefit.

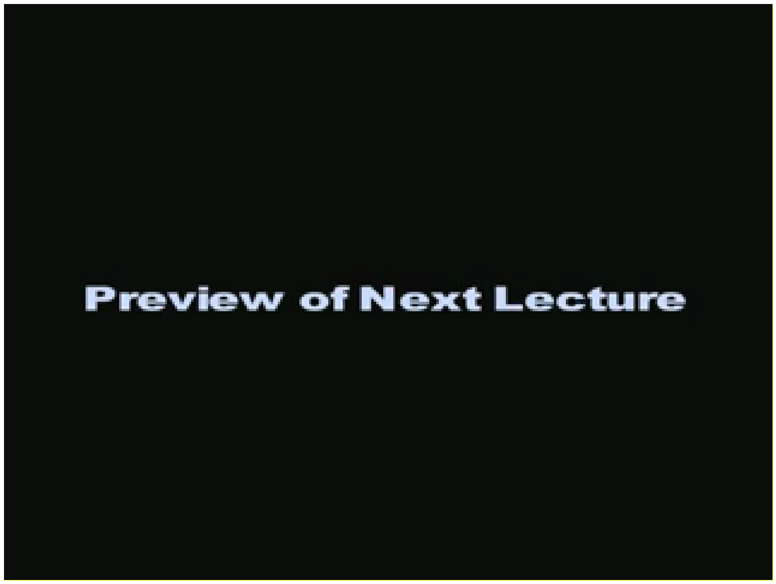
As a matter of fact, in a LAN, you will find that apart from the network boxes (in Greenfield kind of situation), the cost of the cable is also significant. Then there is a question of scalability. Often what people will do is that, they will work with one kind of network and then, very soon, the network will get choked or people will want more bandwidth or more users will join. This keeps on happening. A network is never a stable thing in any organization; but whenever you are putting some kind of topology or some kind of technology you have to think those 3 years to 5 years down the line, you will have to scale the network up. You may have to change the number of your network boxes; some of the boxes for example in old technology you may have had a bus.

By putting in a hub it was a physical star, but it is a bus now. You put a switch over there and make it a star topology kind of thing and then later on people want more bandwidth. When more people want to join, you have to design your physical topology that way for scalability; the bandwidth capacity and the ease of installation because how you take the cables around and how you scale up down and how you can install it are always problems. Ease of finding fault is another important factor. We will talk more about it in the next class. It is good to have a central cabling plan where all cables are coming. You can manage all your cables in one central place .There are standards like structured cabling which are used for easy fault finding and maintenance.
Thank you!

Preview of next lecture

Good day! Today we will be talking about multiplexing.

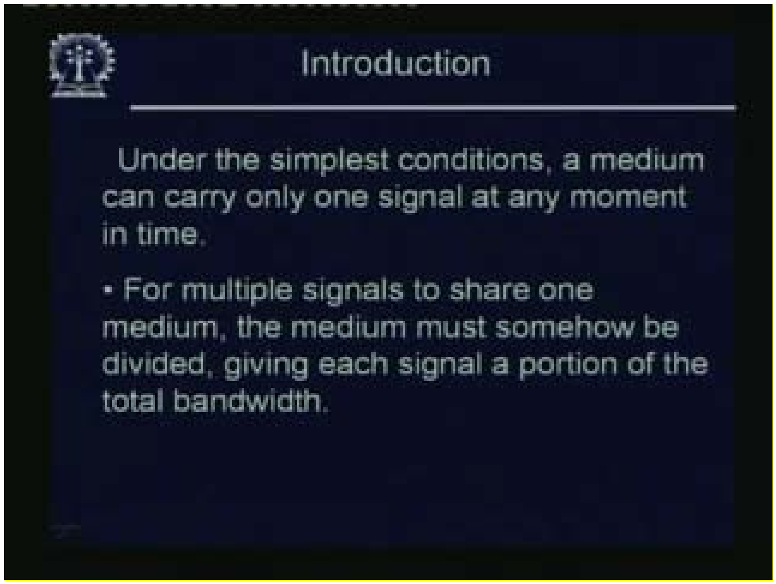
(Refer Slide Time: 51:15)




(Refer Slide Time: 51:25)

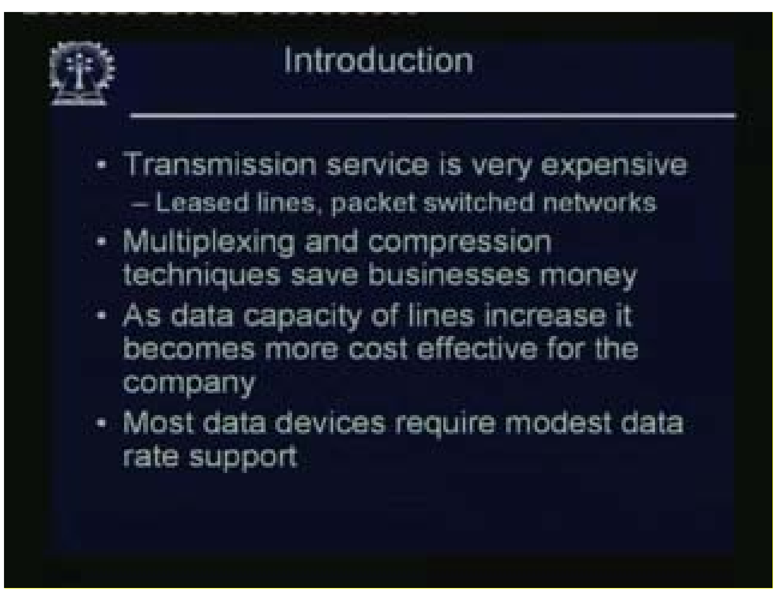

Multiplexing is about sharing a medium. Different users share the same medium for communication at the same time.

(Refer Slide Time: 51:40)



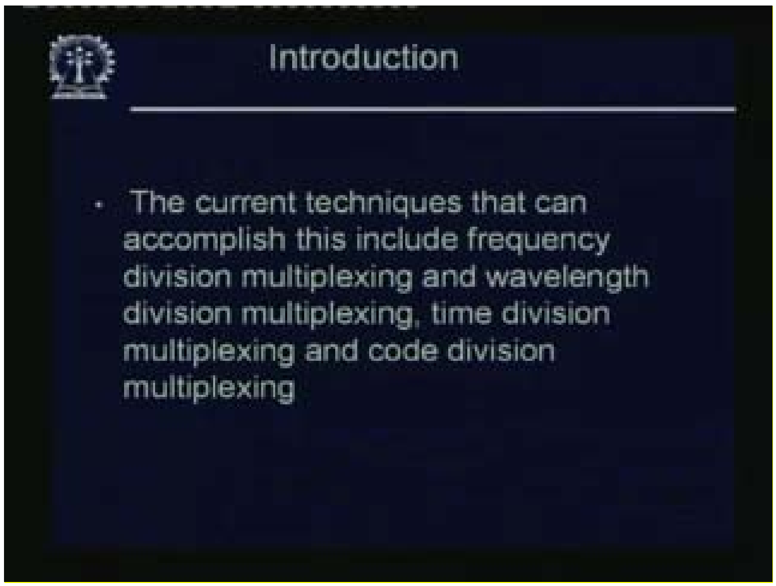

A medium can normally carry one signal at any moment because if there are two signals over there they are going to interfere and then the signals will get garbled .For multiple signals to share one medium, the medium must somehow be divided to give each signal a portion of total bandwidth. A particular frequency range around one particular frequency is called bandwidth and this bandwidth is the most valuable resource as far as communication is concerned. We try to use this bandwidth somehow to facilitate the communication between a number of pairs of senders and receivers. That is the idea of multiplexing. There are various reasons why we want to use multiplexing and the chief one is that of transmission services which are very expensive.

(Refer Slide Time: 52:43)



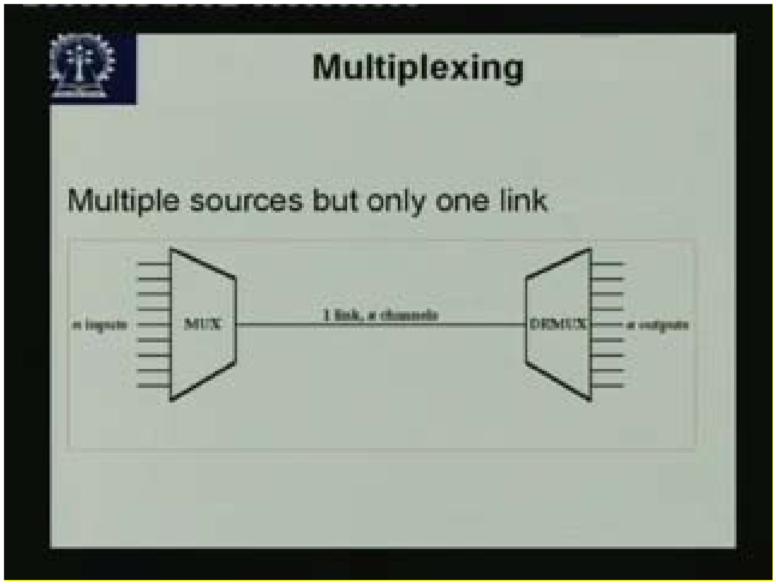
In leased lines packet switched networks, for example, laying of line in itself fairly expensive and complex proposition and once you lay a line you really like to utilize it to the maximum. The other thing is that, if you can use that for the maximum amount of communication multiplexing and compression techniques save a lot of money for the business. When you can send a lot of data through the same line the data capacity of the line increases it becomes more cost effective for the company .Most data devices individually require modest amount of data but with a number of users their aggregated requirements may occupy quite a substantial bandwidth.

(Refer Slide Time: 53:52)



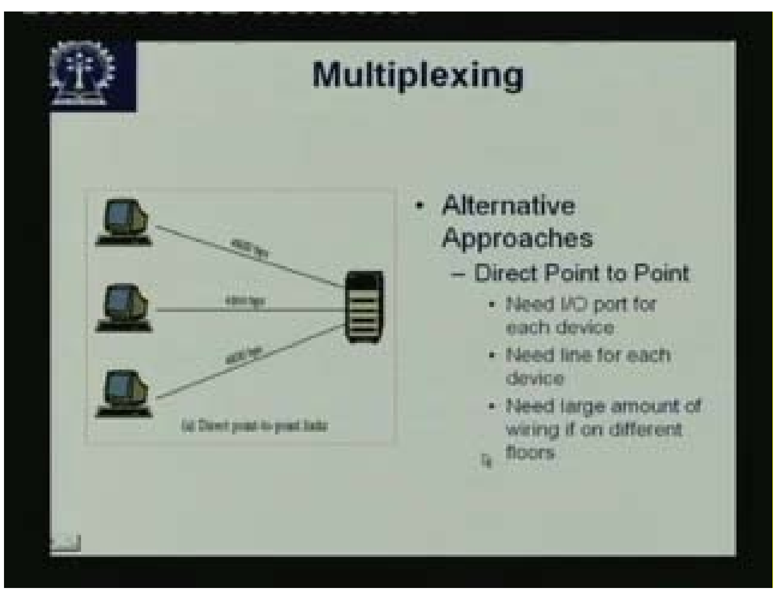

The current technique to accomplish this includes frequency division multiplexing, wavelength division multiplexing, time division multiplexing and code division multiplexing.

(Refer Slide Time: 54:04)



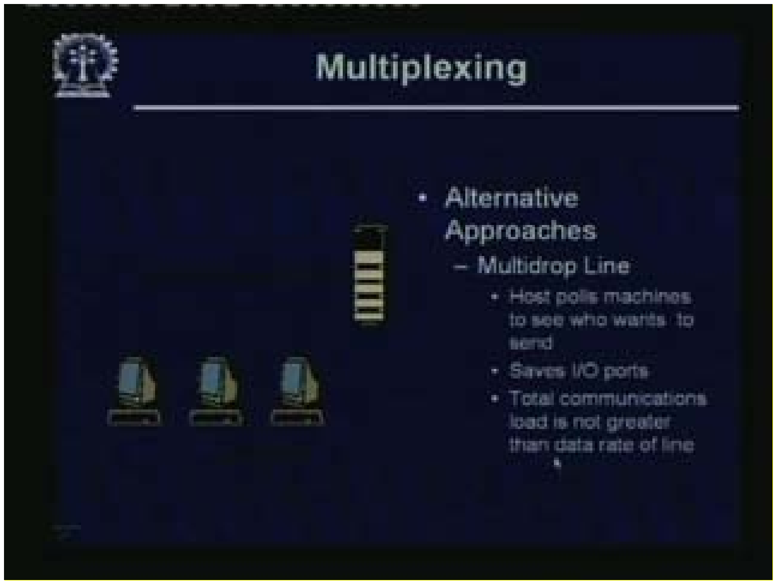

In the scheme of multiplexing, you have one multiplexer and then you have n inputs on one side .So these n inputs are coming to the same multiplexer. They are getting mixed in some fashion and they are being sent over the same physical link .On the other side, depending on how you have put them together, they are separated into different lines. These different lines can now go to different recipients. On the left we have different senders and we have different receivers over here. A number of sender receiver pairs are utilizing the same physical link in between the alternative to multiplexing should be direct point to point connection.

(Refer Slide Time: 54:50)



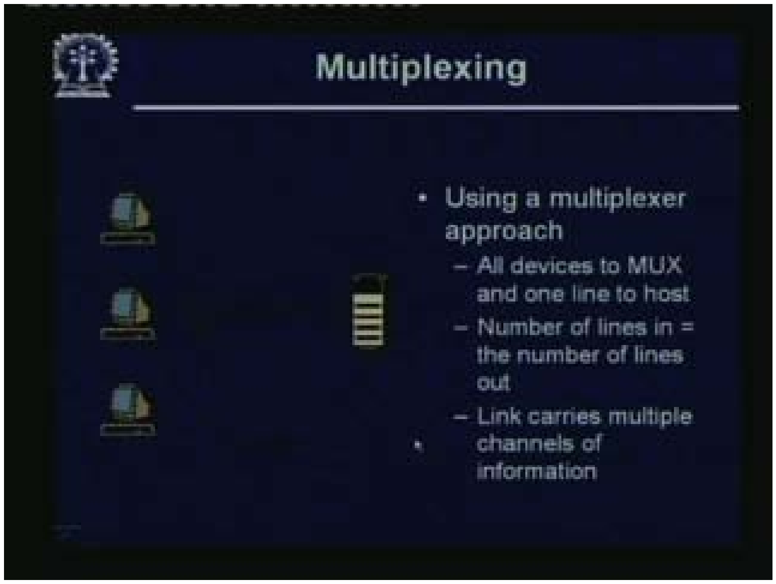
This has number of problems .First problem is that you need those lines that we need for each device. You thus need a large amount of wiring. If they are on different floors, you need large number of IO ports on the computer side, which really is not feasible. You may have a few IO ports, but you cannot have hundreds of IO ports. It is really difficult to have hundreds of IO ports .That is also another bottleneck.

(Refer Slide Time: 55:33)



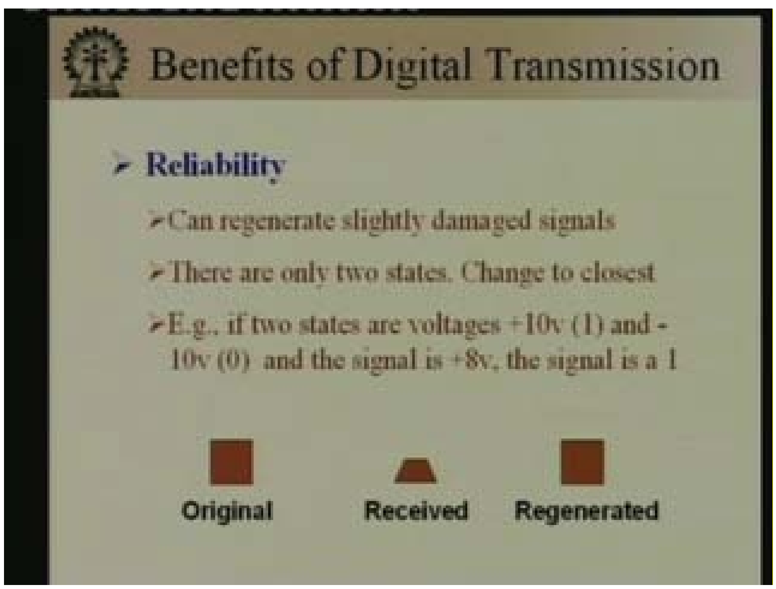

In a somewhat older approach (multi drop line), the host polls machine to see who wants to send and then uses the same lines. Total communications load is not greater than the rate of line.

(Refer Slide Time: 55:55)



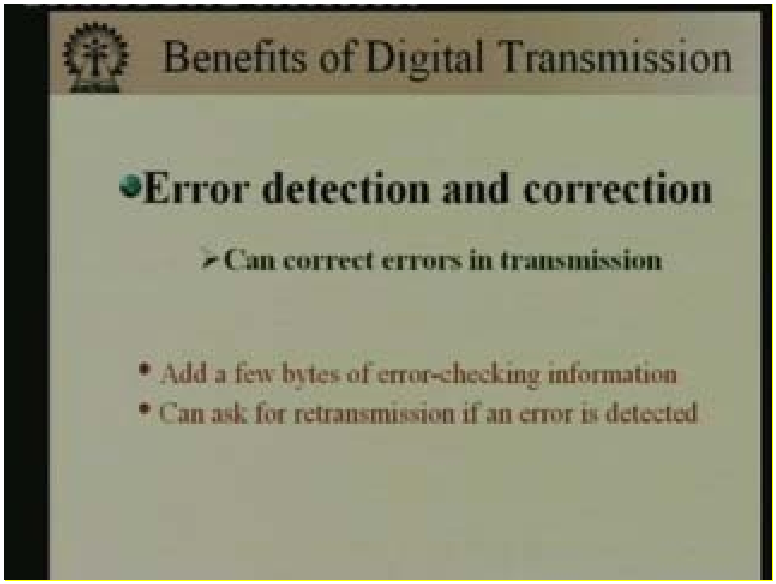

Using a multiplexer approach all the device data's are multiplexed on one side, sent through one a line. Out link carries multiple channels of information the signal will be restored depending on the quantum of noise present.

(Refer Slide Time: 56:16)




If the noise is high then we will lose some information. There will be some distortion and some loss of information would be there. In case of digital signals it is more faults tolerant and more resilient compared to analog signals.

(Refer Slide Time: 57:01)




We can correct errors in transmission. Using digital signals we add few bytes of error checking information and can ask for retransmission if an error is detected. I will give you  a simple example : suppose we are sending groups of eight bits called byte Now what can we do is that associated with each byte we can add an extra byte and this extra byte would make  the number of ones in whole nine bits to be odd . This is an example of odd parity. Now if at the receiver end we find that the number of ones have become even we know that, some bits must have flipped that means some bits must instead of zero have got a one and instead of one we got a zero. It must have happened otherwise because the number of bits are supposed to be odd and of course by adding one bit we can always dictate that the number of bits in the original. That means the sending station was odd .In that case the receiver may request the sender to retransmit the whole bunch once again hopefully there will not be error next time this is of course a very primitive kind of error checking. There are more sophisticated error checking methods employed in networks and communications.

(Refer Slide Time: 58:40)