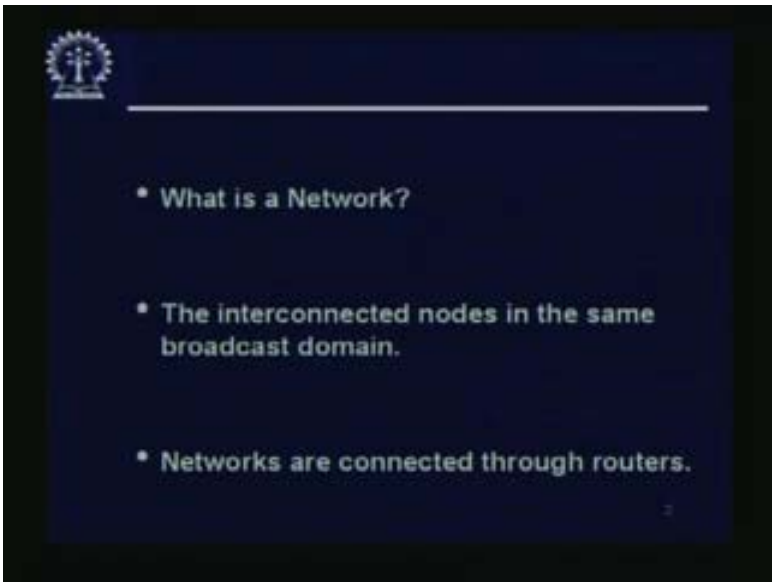
Computer Networks
Prof: Sujoy Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture - 21
Local Internetworking

Good day. Today we will be talking about Local Internetworking What is Internetworking? Internetworking is the connection of different networks.

(Refer Slide Time: 00:51)

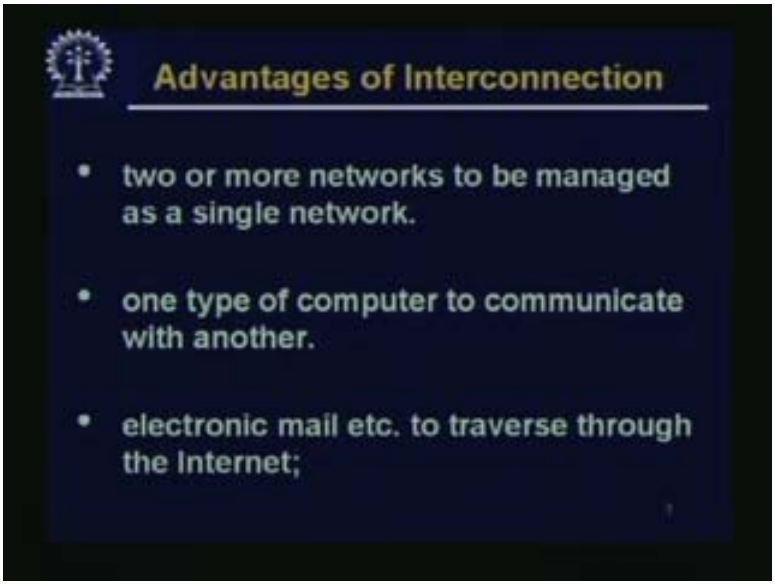
Everybody is aware of the term internet today. Internet comes from this term Internetworking, and by Internetworking we mean connecting different networks.

(Refer Slide Time: 01.13)



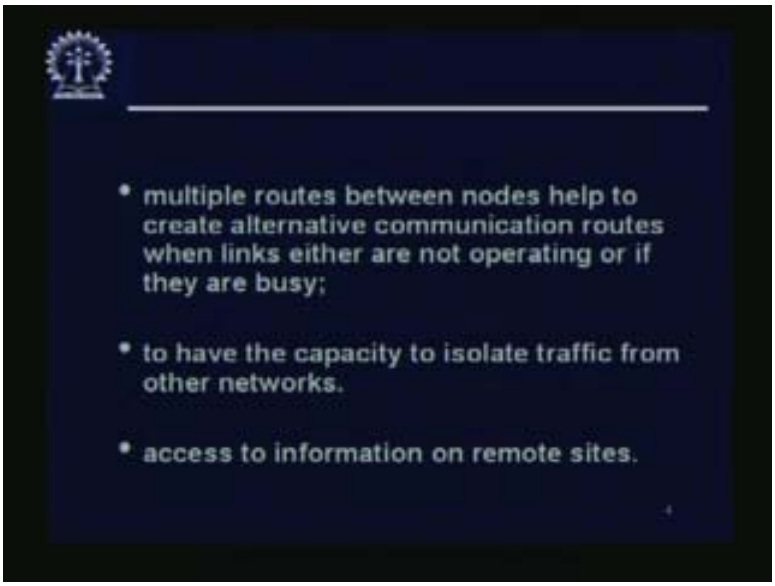
What is a network? As we discussed in the last lecture, the interconnected nodes in the same broadcast domain form a network, and they are usually connected through routers. But for local internetworking, we may not need a router. We may need something called a bridge. Thus, a network is the set of nodes, which are in the same broadcast domain. This broadcast is advantageous for some applications, but for the operation of the network, a crucial requirement is the broadcast. That is used to discover the MAC addresses of the different computers. You can send an ARP message and get the MAC, which will give the IP address. That means you are basically finding out the MAC address of the machine whose IP address is given. The machine will then reply with its own MAC address. That MAC address has to be put in the destination address of the data link layer frame.

(Refer Slide Time: 2:47)



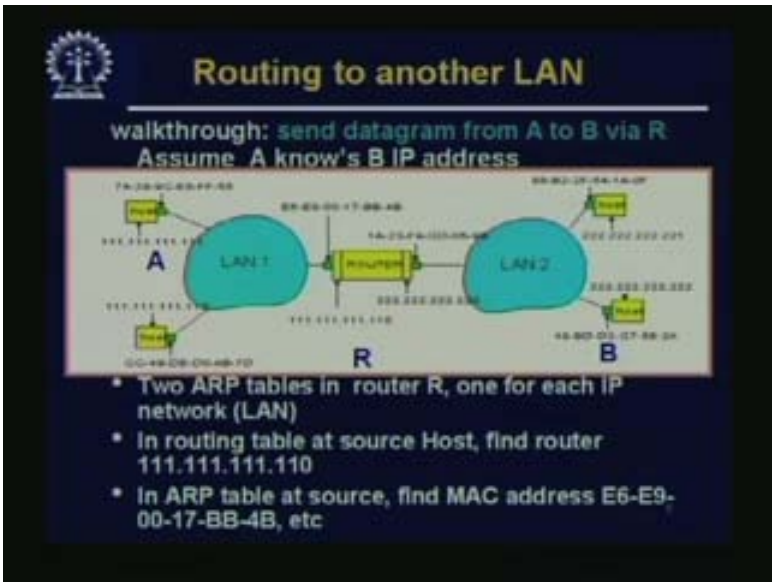
This is how it operates in the single network. If you have two networks which are connected to each other, internetworking is required for so many reasons: two or more networks can be managed as a single network. That could be one advantage of interconnection. Similar type of computers can communicate with another; that is electronic mail, etc., going across the networks. This is another advantage.

(Refer Slide Time: 2.52)



If you have two networks connected, there may be multiple routes between nodes, which help to create alternative communication routes, when links are either not operating or they are busy. The one important reason for local internetworking is to have the capacity to isolate traffic from other networks. As we have seen, if you want to find the MAC address, you send an ARP broadcast. But if the network is large, many people would be broadcasting and the broadcasting load on the entire network will become very heavy. So as the network grows, as more and more nodes and more and more computers get connected to the network, at some point of time, the performance will be getting degraded because so many nodes are sending broadcast messages. The network has to be broken, although it may be in same building. So the scope of broadcast becomes limited.

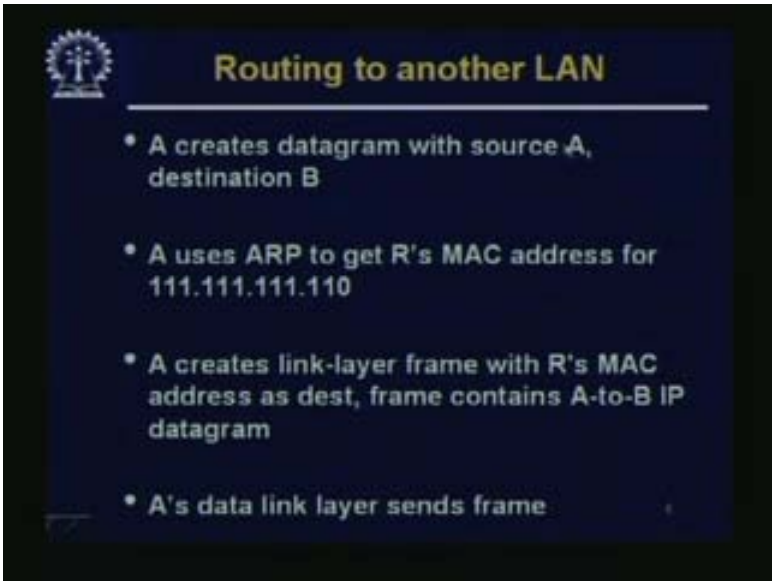
(Refer Slide Time: 04:19)



To have the capacity to isolate traffic from other networks – here we are referring to broadcast traffic – and to access the information on remote sites are the advantages of connecting networks. Look at the problem, which we had glimpsed earlier. Suppose there is this node A, which wants to send a message to a node B. A knows B's IP address but they are in two different LANs which are separated. Nevertheless, they are connected through a router to have some physical connection. A router is some kind of network device that enables two different LANs to communicate with each other. We will see what actually this router does and whether the same thing applies to the bridges. When we come to bridges we will discuss the basics of a router and what it contains and other details when we discuss the network layer. But right now, we will just talk about the ARP and the MAC layers. So let us say that there are two ARP tables in router for this LAN and another one for that LAN.

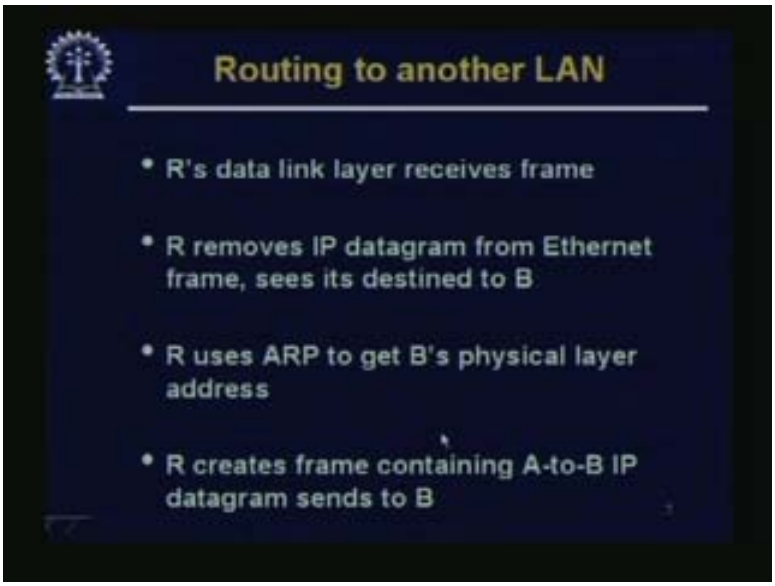
So there are two ARP tables in the router, one for each IP network. In routing table at source host, it has to find the router. First of all, the host must find the router. For finding the router it once again must know the MAC address, which is given over here as something like E5 or E9 etc., which does not make too much sense to human beings. It is just a bunch of bytes, 6 bytes actually. So the host, that is, A, has to know the router in order to send it to B; or in order to even know the address of B, A must somehow communicate with the router; and for communicating with the router it must know the router's IP address. But finally, these two hardware adapters should communicate. So they have to know each other's hardware address or MAC address. It will find the MAC address in the ARP table at source. If it has already communicated with the router, the address may already be in its ARP table. It will do an ARP and find out the MAC address of the adapter of the router.

(Refer Slide Time: 06.51)



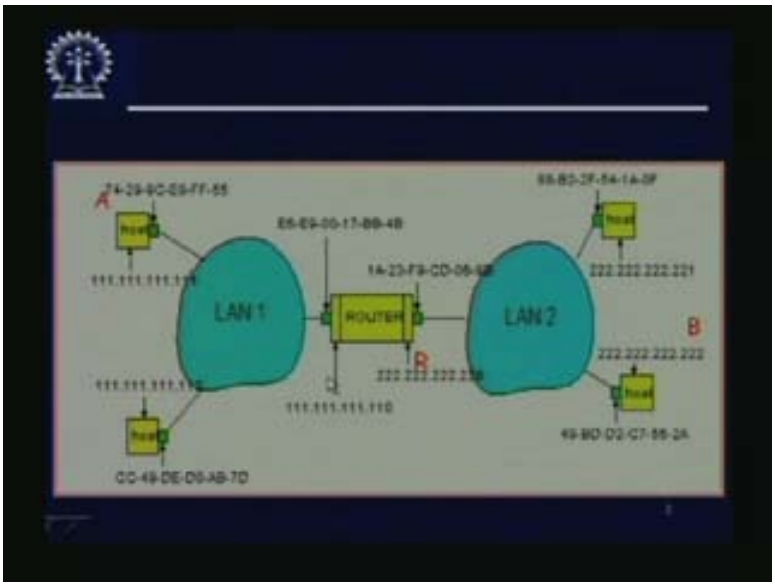
Then A creates a datagram with source A and destination B. Here source A and destination B mean the IP address of B and IP address of A, i.e., the network layer address. This should all be in the packets, which are coming down from the network layer. A uses ARP to get R's MAC address for this. A creates link layer frame with R's MAC address as destination; the frame contains A to B IP datagram; A's data link layer sends the frame.

(Refer Slide Time: 07.23)



R's data link layer will receive this frame on that particular adaptor. R removes IP datagram from the Ethernet frame. Now it is stripped of the data link layer header and trailer and the router sees that this is destined to B. By looking at the IP address, the router would know that it is not in LAN 1 but in LAN 2. So R uses ARP to get B's physical layer address. Now through the other adapter, R must communicate with LAN 2 and specifically to B. For that, it has to know B's address and for that, it does an ARP in LAN 2. Then R creates a frame containing A to B IP datagram, and sends it to B.

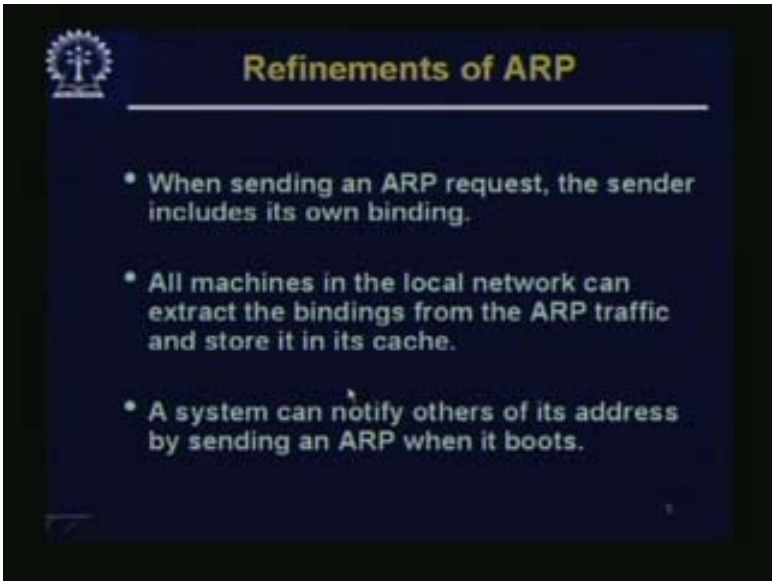
(Refer Slide Time: 08.10)



In this way, A communicates with B and the original packet contains the source IP address as this may be the IP address of A and the IP address of B. This is just for example, and these numbers don't matter. There is a 4-byte IP address and that datagram is sent with A's source MAC address to the router. Router finds the MAC address as destination B, does the ARP in the LAN 2 and finds out the MAC address, which is 49B-D. Then R forms the net frame,

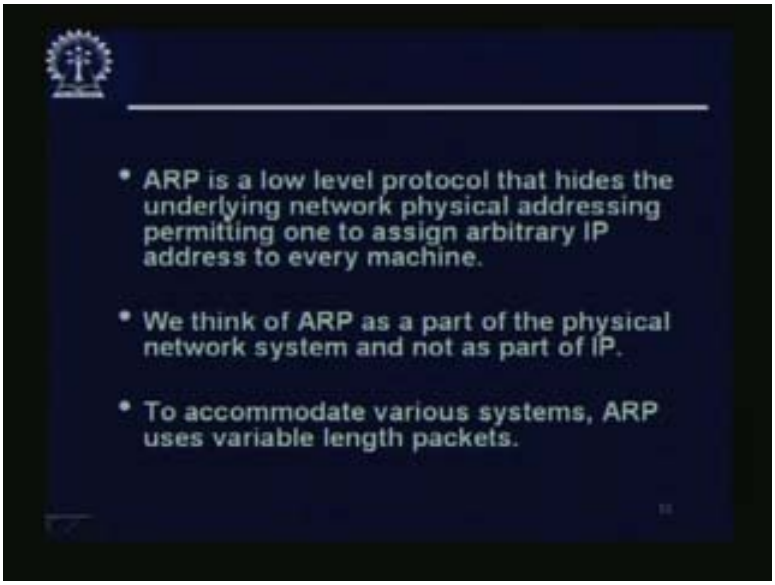
which contains the original packet which was sent by A's network layer. But now it has the source as the MAC address of the router and it sends it to the MAC address of B through the LAN. This is how the whole scheme works.

(Refer Slide Time: 09.11)



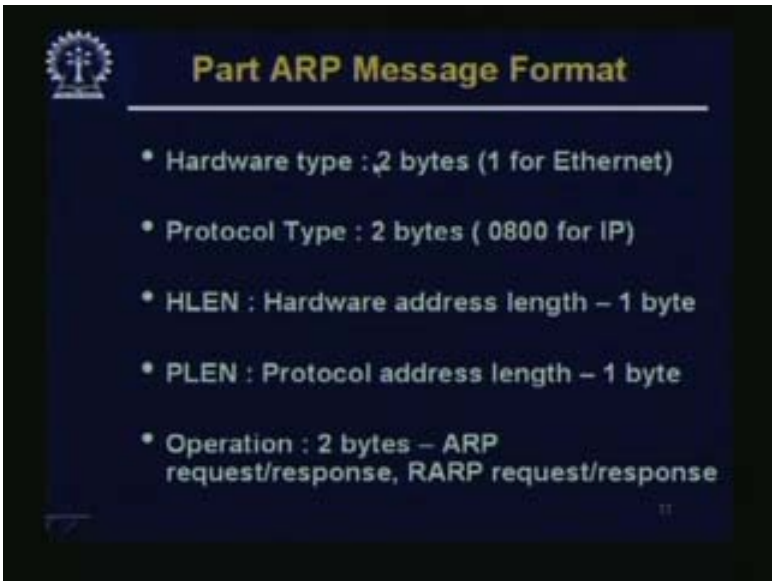
We will see just a couple more slides for finishing this ARP. When sending an ARP request the sender includes its own binding; that means, its own IP address and MAC address. All machines in the local network can extract the bindings from the ARP traffic and store it in its cache. Remember all other nodes don't have anything to do with this ARP, but still they listen to this ARP traffic, which is going on and whatever bindings it can, it extracts and puts it in its cache, so that if this particular machine wants to communicate with any one of those, it can bypass the ARP and get it straightaway from the ARP cache, rather than doing a broadcast on the network again. A system can notify others of its address by sending an ARP when it boots, because it includes its own binding in the ARP message.

(Refer Slide Time: 10.19)



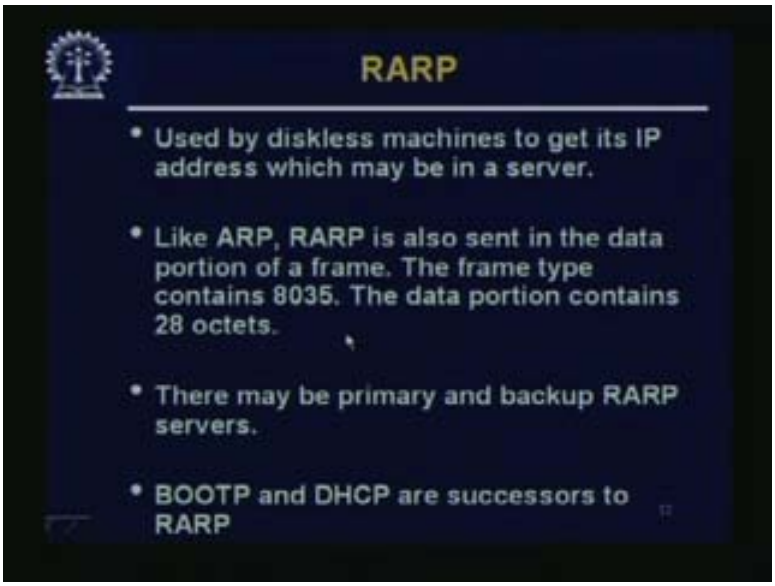
ARP is a low-level protocol that hides the underlying network's physical addressing, permitting one to assign arbitrary IP address to every machine. We think of ARP as a part of the physical network system and not as part of IP. So, ARP has to do more with the data link layer rather than the network layer. The other protocol, which is predominately related to the IP address, will be discussed later. To accommodate various systems, ARP uses variable length packets because these ARPs may be used in different networks

(Refer Slide Time: 10.57)



So this is just a part of ARP message format; there are other parts of it. The format used is, Hardware type: 2 bytes. (For example for Ethernet you will get a value of 1), Protocol type: 2 bytes (0800 for IP), Hardware address length: the ARP may be used in various networks and various networks may have different classes of hardware addresses, which are of varying length. If it is just the Ethernet address, there will be 6 bytes but for other kinds of networks it may be something different. So the hardware address length mentioned here is 1 byte; protocol address length is mentioned in 1 byte; but operation is 2 bytes of ARP; i.e., it could be ARP request/response, RARP request/response, etc.

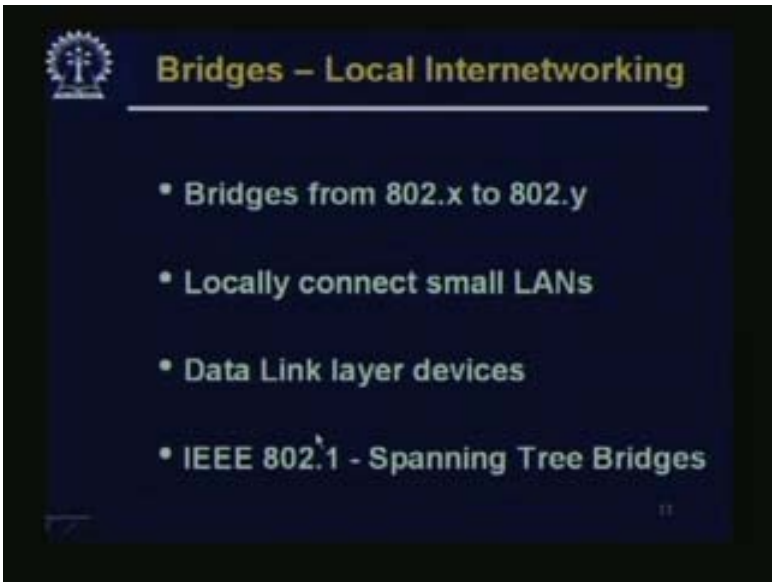
(Refer Slide Time: 12.08)



What is RARP? RARP stands for reverse ARP. What is ARP? ARP is used to find the MAC address of the machine having a particular IP address and RARP is the reverse. What is the IP address of the machine having this particular MAC address? RARP is required to know one's own IP address, when one can't store one's IP address locally and specifically. One place where it is quite often used is in diskless machines. Nowadays, there is a concept of diskless machines and they are also known as thin clients, which use the computational power and the disk storage, etc., of a central server. These thin clients, since they have minimal functionality, are easier to maintain. It may be a little cheaper to upgrade them, as it is easier to upgrade one central server rather than a whole bunch of PCs. So, if you have a thin client and a server in a network, they communicate with each other in an IP network.

But for communicating, for being an entity in the IP network, you must have an IP address. How is this IP address to be stored in this diskless machine, which does not have any disk, to store anything permanently? Whenever you switch it off, all of it becomes volatile, except for the small ROM. So when it boots up, it has small program in its ROM, which can do some elementary processing. It can find out its own MAC address because it is just local and give that MAC address with an RARP, asking for its own IP address and the server will assign an IP address to it. So RARP is used by diskless machines to get its IP address, which may be in a server. Like ARP, RARP is also sent in the data portion of the frame. The frame type contains 8035 and the data portion contains 28 octets. There may be primary and back-up RARP servers. There are two other protocols like BOOTP and DHCP, which are successors of RARP, and they have to do more with the network layer. We will talk about BOOTP and DHCP later, when we talk about the other TCP/IP protocol suites.

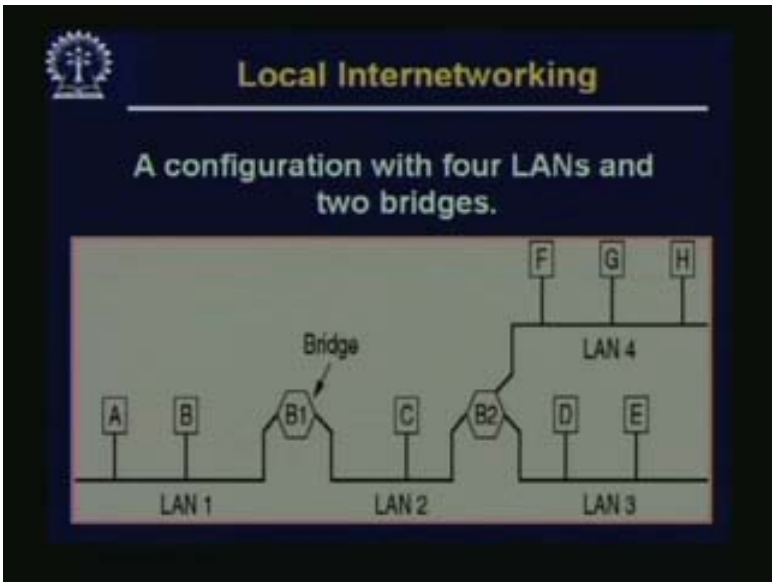
(Refer Slide Time: 14.51)



Till now, we have seen what internetworking is; it means connecting two different networks together. If this internetworking is local, i.e., may be in the same organization or may be in the same building or in nearby buildings, in the same campus, etc., you may not require the full power of a router for the networking part. You may do it with a data link layer device, called a bridge. We will be discussing about bridges today. Bridges can connect different networks. As a matter of fact, they can connect different networks of different types. For example, a bridge can connect 802.x to 802.y.

These x and y may have the same value; i.e., both of them may be 3, that is, both of them may be Ethernets or one may be an Ethernet and another may be a Token Ring, something like locally connected small LANs. If a LAN is big, bridges can't handle it any longer. It is a data link layer device and it follows a protocol from IEEE 802.1, which is a spanning tree of bridges. If you remember how this IEEE 802 protocols are organized, 802.1 is put at the top as it gives an overview and a few things which are generally applicable to all the layers. Then we have 802.2 for link layer, etc., and 802.3 is Ethernet 4 for token bus, token ring, etc. So we will look at some more 802 protocols when we discuss wireless networks. A bridge may connect different types of networks and that is why it is put in 802.1; this uses spanning tree protocol. We will discuss the spanning tree protocol presently.

(Refer Slide Time: 16.52)



A local internetwork picture would look something like this. Suppose there are four LANs: LAN 1, LAN 2, LAN 3 and LAN 4, which are connected by two bridges. Bridge has two ports – one connecting to LAN 1 and the other to LAN 2. Bridge has three ports, each one connecting to LAN 2, 3 and 4. Now, A can communicate with H through two bridges.

(Refer Slide Time: 17.21)

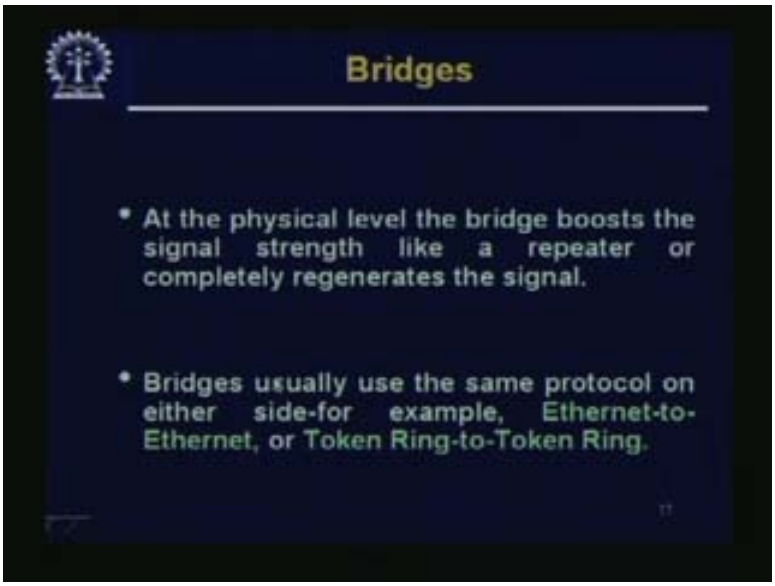
Let us see the salient points of a bridge. First of all, it is a link layer device. It stores and forwards Ethernet frames, which means it is related to the MAC address rather than the IP address. These bridges handle the hardware addresses. It examines frame headers and selectively forwards frames, based on MAC destination address.

This means that (in the previous diagram) when gets some frame from here, it will look at the hardware address and decide whether to send it to LAN 4 or to LAN 3. It would selectively send it to one of them. When the frame is to be forwarded on segment, it uses CSMA/CD to access the segment. So that is the protocol.

(Refer Slide Time: 18.19)

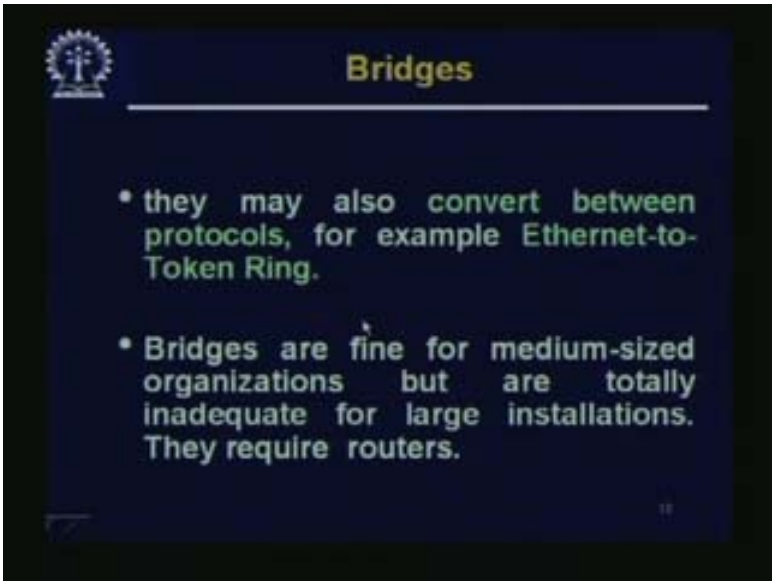
Bridges are transparent, that is, hosts are unaware of the presence of bridges. To the host the whole thing might look like one single network. Since it is transparent and plug-and-play device, it will do some self-learning and start operating. In the beginning of the self-learning phase, it may be little inefficient but later on its efficiency will improve as it learns more. Bridges need not be configured, which is another advantage. A bridge separates LANs if we want each group's traffic to remain within its own LAN. There are other reasons like security issues to maintain the traffic within one's own LAN.

(Refer Slide Time: 19.47)



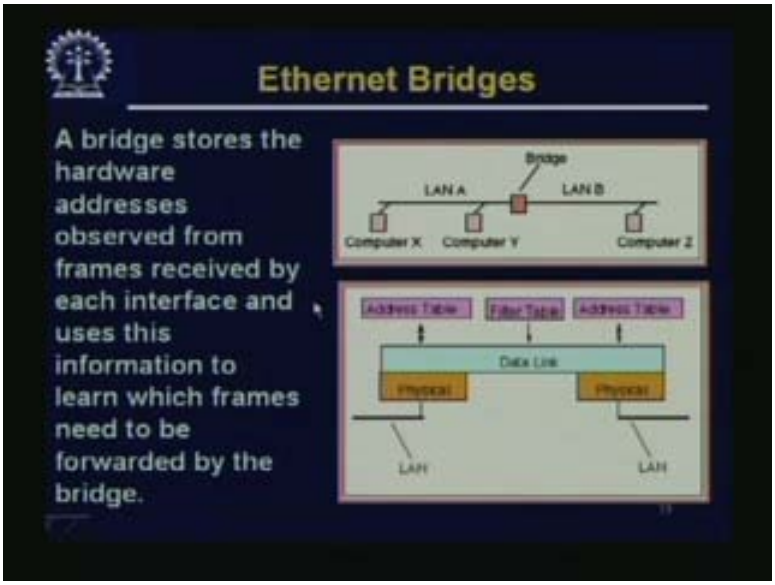
At the physical level, the bridge boosts the signal strength like a repeater or completely regenerates the signal. Just like a hub or a switch, before forwarding the signal, it will boost up the signal, i.e., the signal is being regenerated, which is highly advantageous. Bridges usually use the same protocol on either side; for example Ethernet-to-Ethernet or Token Ring-to-Token Ring.

(Refer Slide Time: 20.13)



They also convert between protocols. For example, Ethernet-to-Token Ring Protocol Conversion is possible in bridges. Also bridges are fine for medium-sized organization but are totally inadequate for large installations.

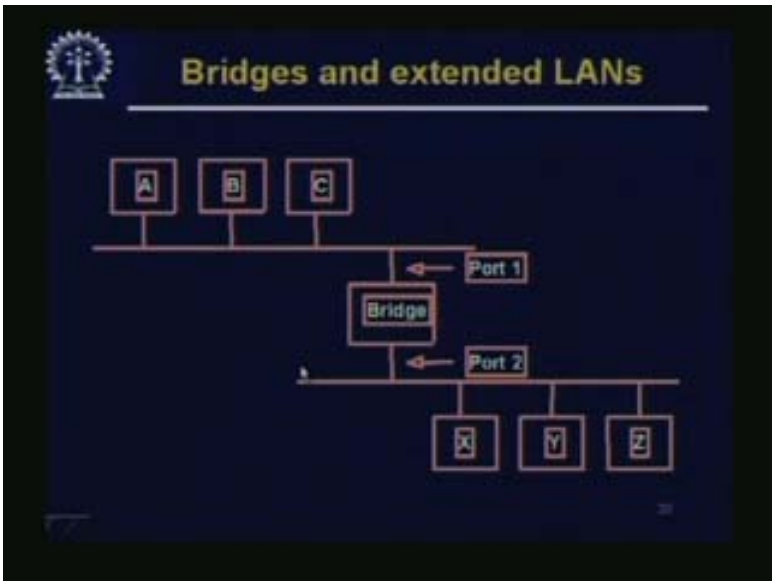
(Refer Slide Time: 20.26)



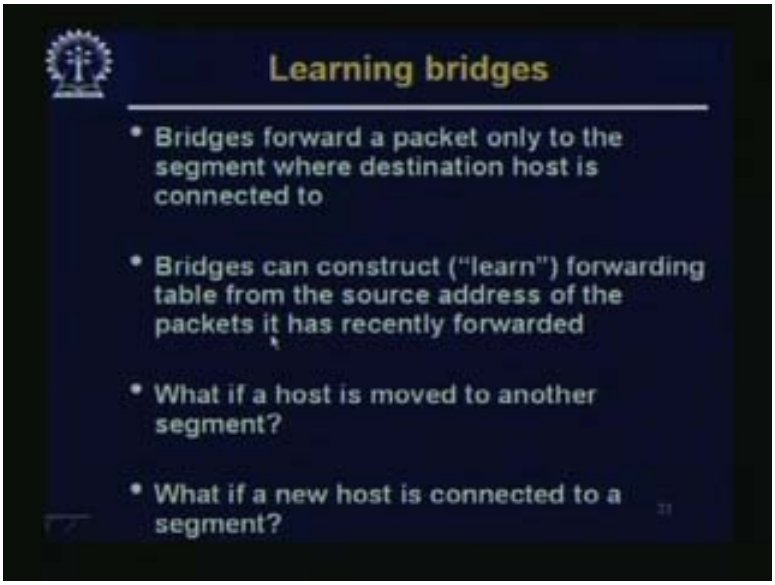
They would require routers a bridge stores the hardware addresses observed from the frames received by each interface and uses this information to learn which frames need to be forwarded by the bridge. It will maintain a table in itself and for each of these interfaces and

in that table it will store all the hardware addresses it has seen in the segment. So it will know the location of the machines in the different segments. If it gets a packet from LAN A, which has a hardware address for the machine in LAN B, it will send it to LAN B. Each bridge has physical interfaces, the data link layer, the address table and the filter table. How is it filtered before being forwarded? Using the information from the address table it learns which frame needs to be forwarded by the bridge.

(Refer Slide Time: 21.28)



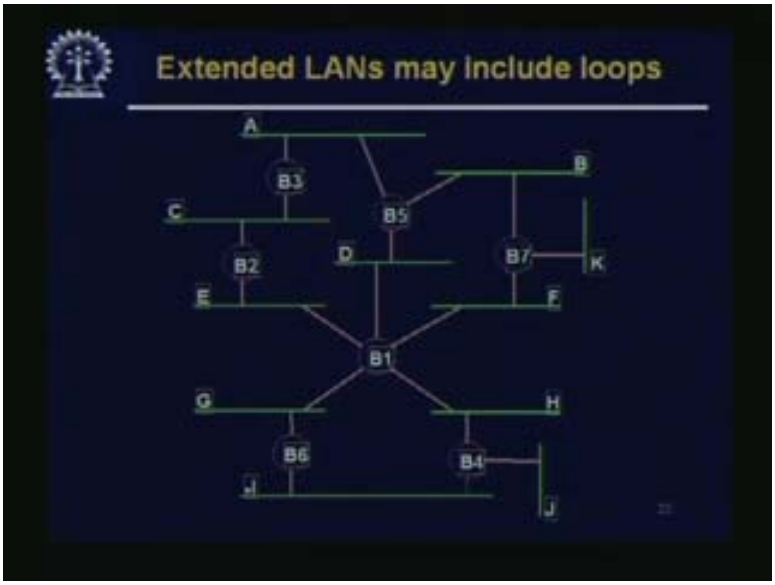
(Refer Slide Time: 21.32)



This is just an example in the form of a picture so bridges forward information only in the form of packets to the segment where the destination host is connected to. Bridges can construct (learn) forwarding table from the source address of the packets which have recently been forwarded to it. So whenever there is an ARP on that side of the LAN, the port of the bridge that is connected to it will also get that ARP request. Then it finds some of the bindings and it quickly learns and fills up its table. What will happen if a host is moved to

another segment or if a new host is connected to a segment? If a new host is connected to a segment, this learning becomes a continuous process. If a system is moved from LAN 1 to LAN 2, the network interface card, which is present in it, also goes along with the machine from LAN 1 to LAN 2. Since the particular MAC address has moved from LAN1 to LAN 2 the table entries of the system moved will get erased and the data remain fresh and relevant.

(Refer Slide Time: 22.59)



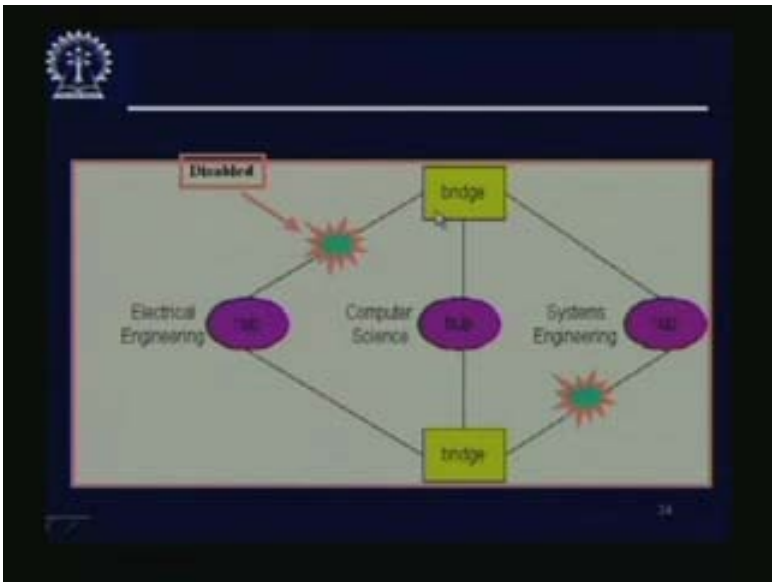
In the above slide, the green ones are the different LAN segments and till are seven bridges and they are connecting multiple LANs. You can connect multiple LANs like this; but it has a problem of looping and now we will discuss how to avoid that.

(Refer Slide Time: 23.40)

For increased reliability, it is desirable to have redundant alternative paths from source to destination. With the multiple paths, cycles result and so bridges may multiply and forward

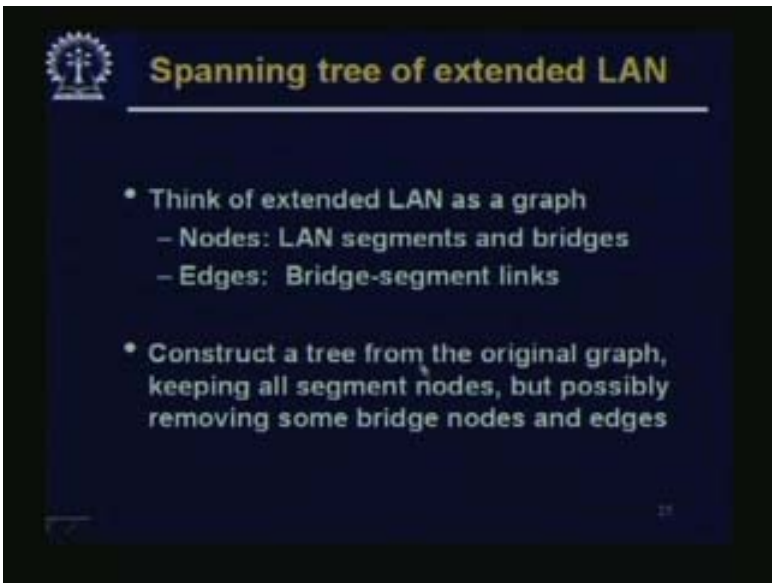
frames forever. The frame may go on and on without a frame getting dropped, because in the bridge and in the data link layer there is no concept of a particular frame moving around for a long time. Since there is no way to handle that, we do it in IP layer. We will discuss about that later. Once the frame starts circulating, that means, going in a cycle, it will go on and on and such frames may actually increase in numbers and then bring down the whole network, which is not acceptable. The solution for this is to organize bridges in a spanning tree by disabling subset of interfaces willfully, in the sense that we don't use them.

(Refer Slide Time: 24.50)



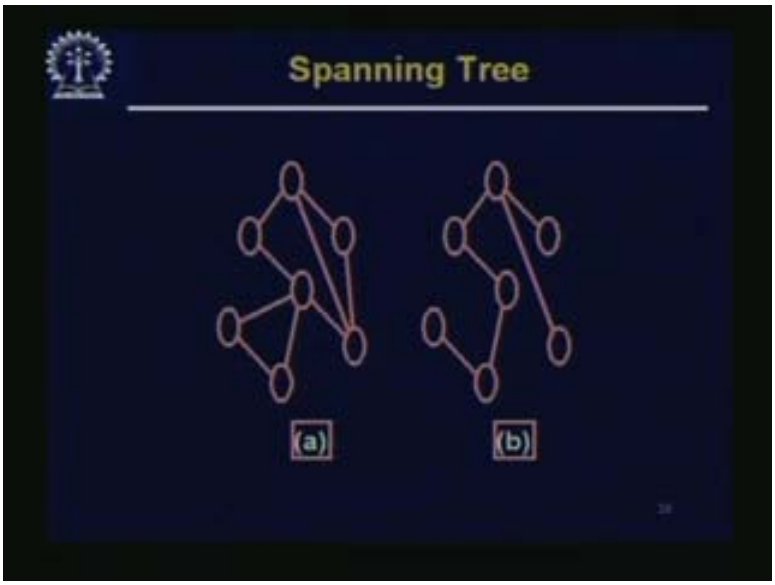
Suppose you have a graph as shown above, there could be cycles over here but if you disable these two interfaces of the bridge, you no longer have a cycle. So with these three paths shown you can't have a cycle.

(Refer Slide Time: 25.13)



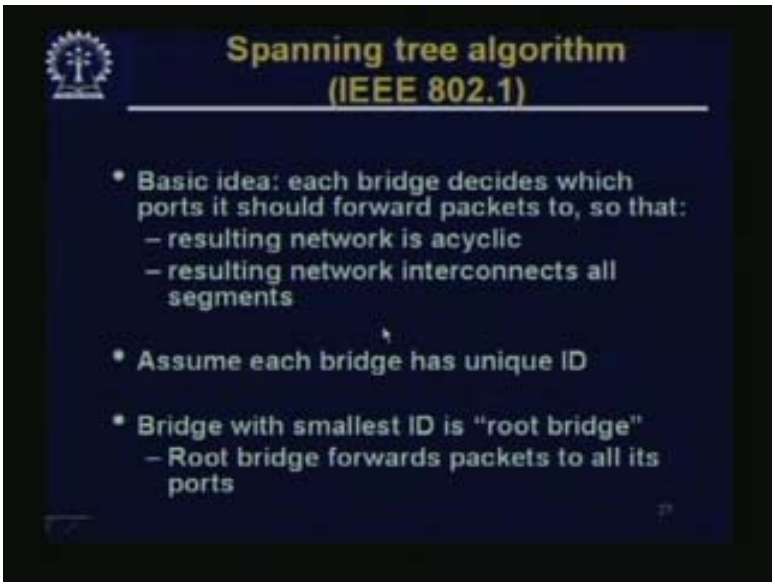
We can think of the extended LAN as a graph. Its nodes are the LAN segments and bridges. Edges are bridge-to-segment links. This is how a graph should be constructed. Now construct a tree from the original graph keeping all segment nodes and removing some bridge nodes and edges. The individual LAN segments are the nodes and for the bridge to the LAN connection, we form an edge. This graph may have cycles. We remove the cycles minimally by still keeping the graph connected. If the original graph is not connected, i.e., if it is not possible to go from one node to another, then in the diagram there is no physical connection and hence you can't do anything about it. But if the original one was connected and when we disable some of the links to avoid cycles, we must keep it minimally connected and so all the nodes are retained. That is why it is called a Spanning Tree. So, finally what we want is to have a Spanning Tree with some of the edges disabled to avoid cycles.

(Refer Slide Time: 26.38)



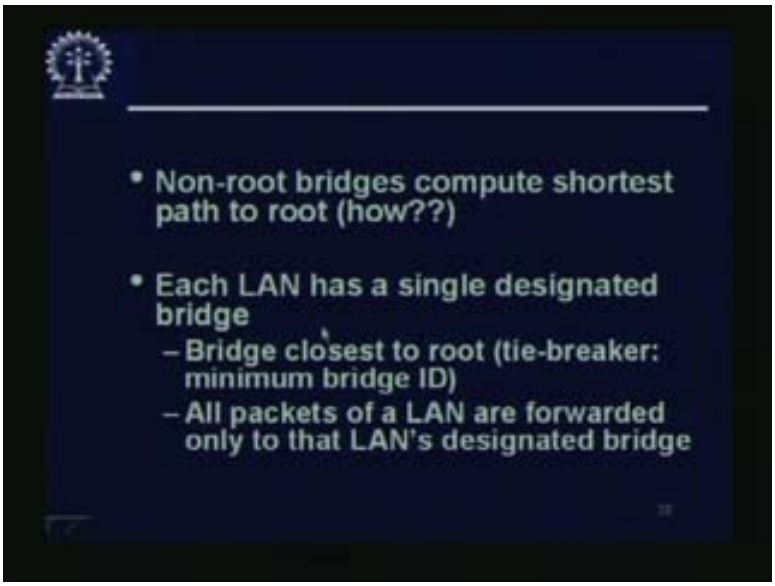
The above slide is an example graph with lots of cycles. We remove some of the edges so that the graph still remains connected and it is still possible to go from any node to any other node without a cycle in this graph. This is the Spanning Tree in which all the nodes are still connected but there is no cycle.

(Refer Slide Time: 27.00)



For this, we use the spanning tree algorithm from IEEE 802.1. The basic idea is that each bridge decides which ports it should forward packets to, so that the resulting network is acyclic and the resulting network interconnects all segments. Assume each bridge has a unique ID and each one knows its own ID. By the algorithm, we assume that the bridge with the smallest ID is the root bridge and this root bridge forwards packet to all its ports.

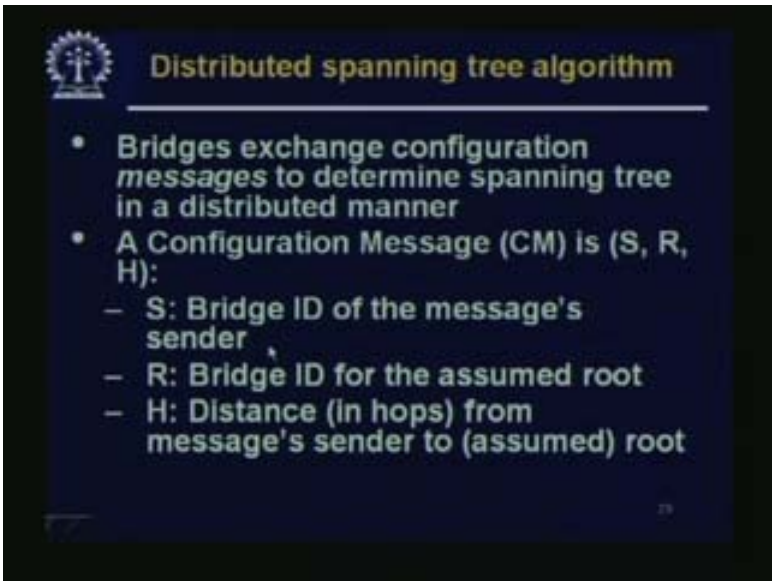
(Refer Slide Time: 27.35)



How do non-root bridges compute the shortest path to root? Some algorithms are distributed algorithms, i.e., each node does some computation using the locally available knowledge. But this locally available knowledge may not be consistent with the global picture as the global picture is not known. Since the local things are known, we go for distributed algorithm instead of a centralized algorithm. We do use centralized algorithm, gather all the information together in one place, and then do the computation. Centralized or traditional algorithms are obviously easier but it is more difficult to write distributed algorithms. But you don't have

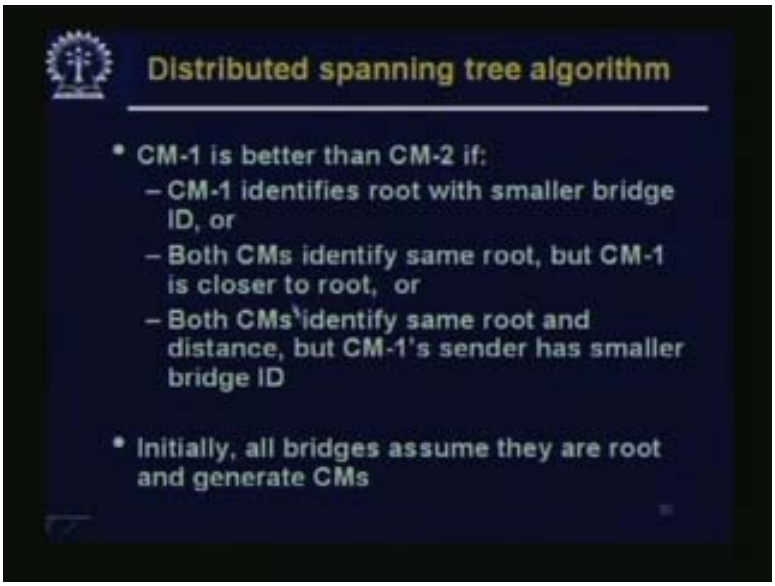
any option. You have to write a distributed algorithm. A node or a bridge in this particular case can do the computation only based on what it knows locally. It does not have the global picture. It tries to form a global picture and that is the task of the algorithm, to form that global picture. Each LAN has a single designated bridge closest to root and the tie-breaker is the minimum bridge. All packets of a LAN are forwarded only to that LAN's designated bridge. We will look at this algorithm in more detail.

(Refer Slide Time: 29.04)



Bridges exchange configuration messages to determine spanning tree in a distributed manner. The configuration message (CM) consists of three things, S, R and H, where S is the bridge ID of the message sender, R is the bridge ID for the assumed root. Whoever is sending this CM, assigns the best value for the root; that is R. H is the distance in hops from message sender to the assumed root, so H is the distance from R to S, as is known to this particular bridge. So CM gives these three things: bridge ID, root ID, and the distance from the root to the particular sender.

(Refer Slide Time: 30.05)



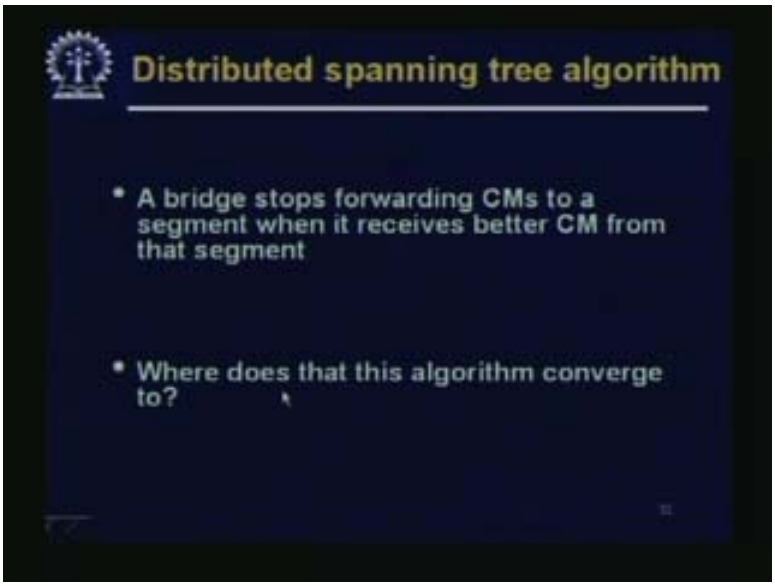
When there are two CMs, we say CM-1 is better than CM-2, under three conditions. When CM-1 identifies root with smaller bridge ID; when both the CMs give the same root ID you can't say which one is better based on this but CM-1 is closer to root; when both CMs identify same root and distance to the root, but CM-1's sender has smaller bridge ID. In these cases, CM-1 is preferred. Initially all bridges assume that they are roots and generate CMs. As the algorithm starts, all the bridges assume themselves to be root and send initiating CMs to all its neighbor nodes.

(Refer Slide Time: 31.27)

Each bridge remembers the best CM it has received or sent. The best CM is the value of the smallest root it has received. If more than 1 value of the root is same, the best CM is the one in which it can reach the root with the smallest number of hops. Bridges use the best CM to determine true root and to compute the distance to root.

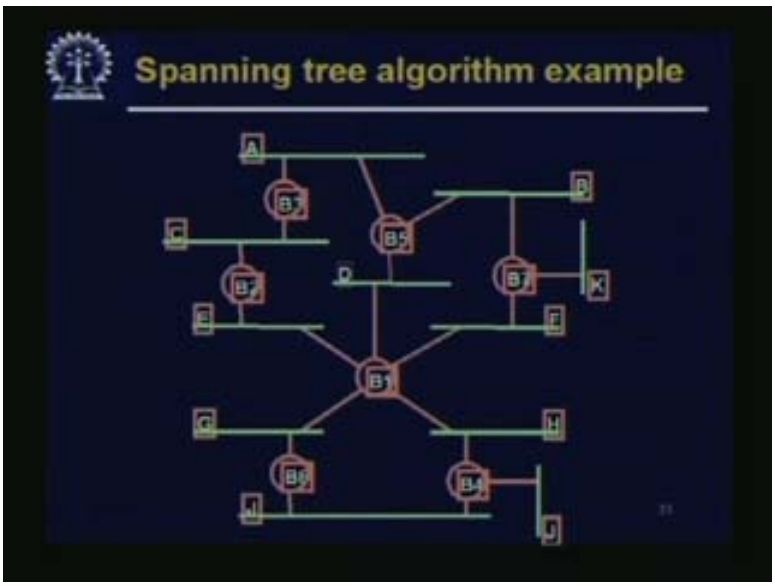
A bridge stops generating CMs when it realizes that it is not the root. After that point, it simply forwards all CMs it receives.

(Refer Slide Time: 32.24)



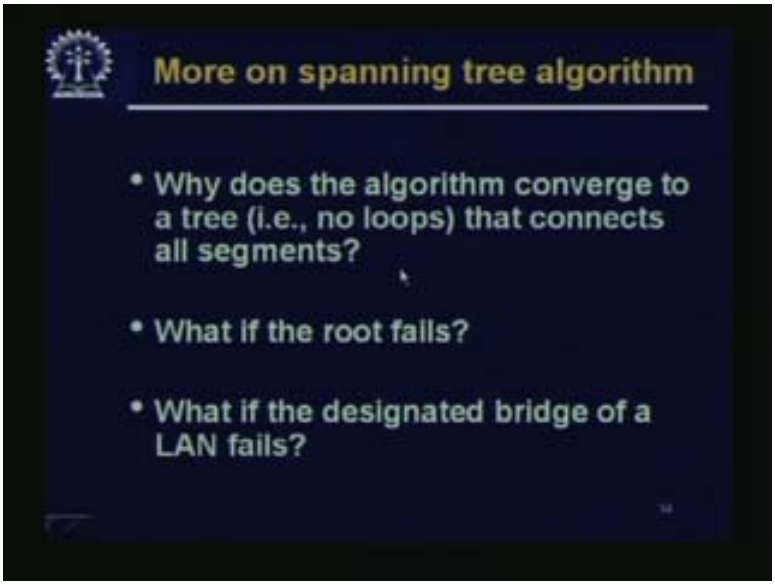
A bridge stops forwarding CMs to a segment when it receives better CM from that segment. Suppose a bridge is sending a CM with some particular root; and through some other segment a CM has come with a better root and the better root and the path to the better root are through the original segment, then that segment will not get CMs forwarded from this particular bridge.

(Refer Slide Time: 33.11)



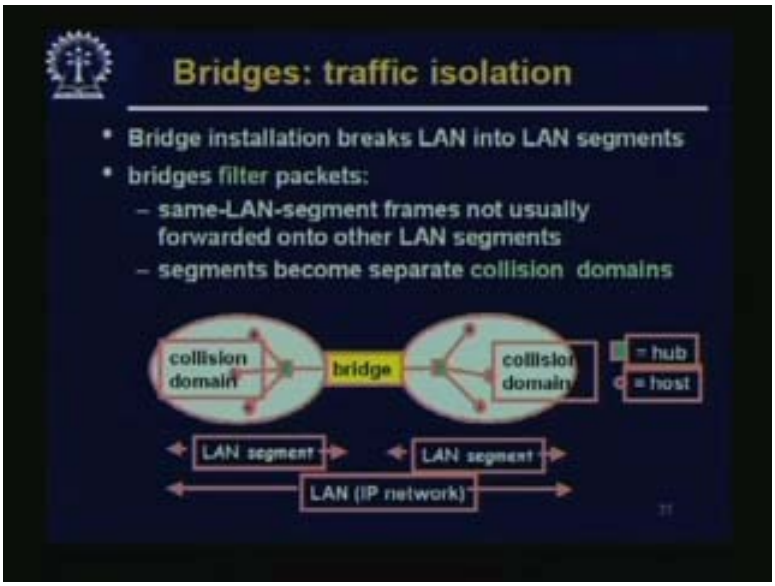
Then where does this algorithm converge to? Let us say will send CMs to and when gets a message from it knows that is on this side and so it will stop sending on this segment. Will send about to But this is two hops away so Will not only know that is there but it will know the shortest route also. Will get the message from either or through ,whichever comes first. So it will find its hop to the root .Then among and , is smaller assuming , , , , , , are in the lexical order. So it will connect to. This is how they all will come to know about the root very quickly. Although each bridge may initially think of itself as a root, at some particular point of time, for example, originally assumes that it is the root but when it gets a CM from, it will know that there is something smaller than itself and must be the root. So it will latch on to . will of course by that time have got the CM from and knows is the root. So it will forward this CM with as the root and with its own distance to and with it to . Now will know that is the root. In this way, all the bridges will come to know about the root very quickly and they will latch on to the path or the root, which goes through the smallest number possible error. For example, could latch through or but it will choose and in this way we will finally have a tree.

(Refer Slide Time: 35.38)



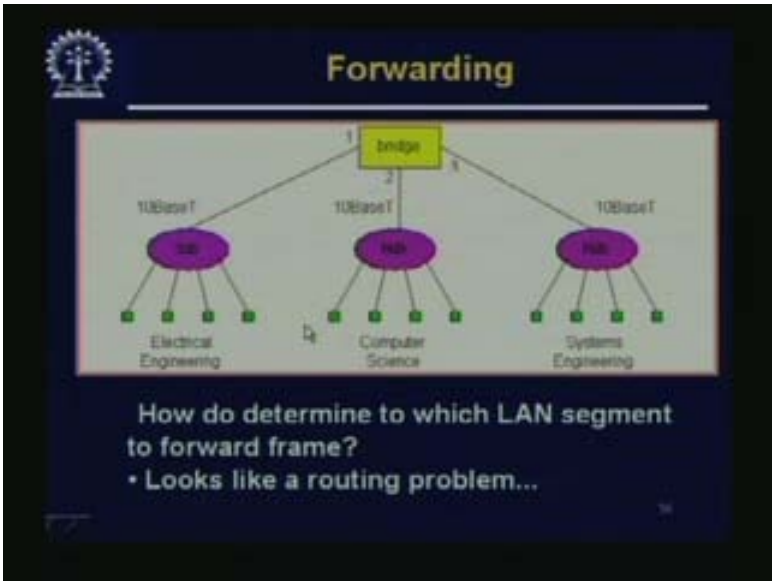
Now the algorithm will converge to a tree that connects all segments. What if the root fails or what if the designated bridge of a LAN fails? To identify these you have to run this spanning tree algorithm from time to time.

(Refer Slide Time: 36.13)



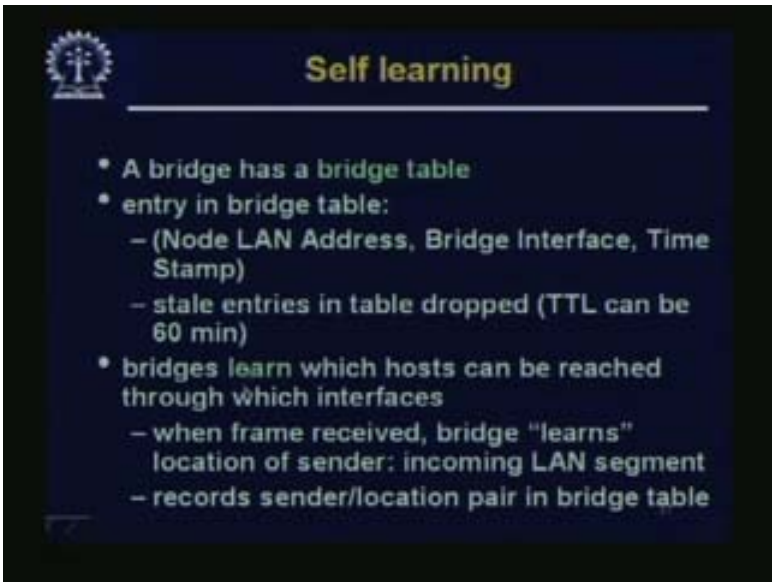
One of the main uses of the spanning tree algorithm is to isolate the traffic, specifically broadcast traffic. So bridge installation breaks LAN into LAN segments and bridges filter packets. Same LAN segment frames are not usually forwarded to other LAN segments. Hence segments become separate collision domains and any broadcast over here is just limited to the particular segment. So this is the full LAN 1 IP network divided into LAN segments which are bridged. There may be hubs, nodes, etc.

(Refer Slide Time: 37.05)



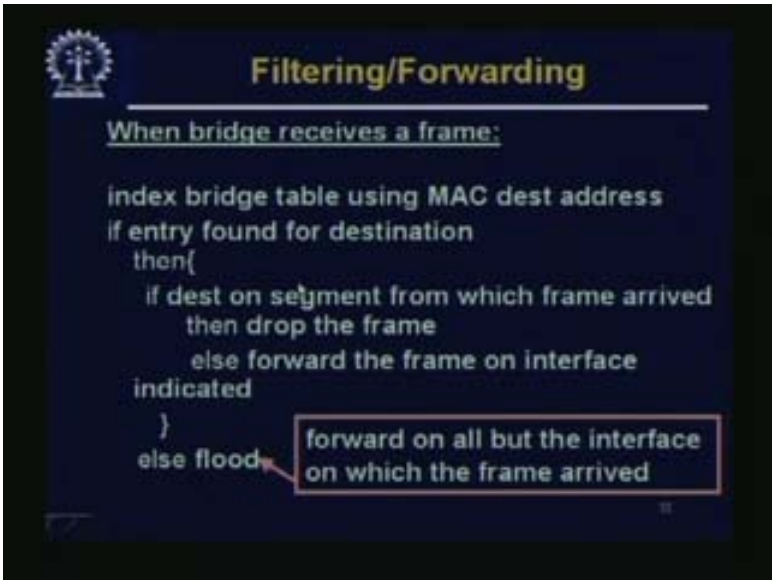
How does the bridge know which LAN segment to forward the message? When a bridge gets the frame how does it know where to forward it?

(Refer Slide Time: 37.20)



A bridge has a bridge table and entry in the bridge table is of node LAN Address, bridge interface and time stamp. The node LAN address is the MAC address, the bridge interface is the group to which it belongs. If the entry in the table becomes too old and is to be dropped from the table, such stale entries in the table can be dropped after a particular prerequisite time known as time stamp, which can be configured (60 min for TTL). So a configured bridge knows which hosts can be reached through which interface without traffic. When a frame is received, the bridge learns the location of the sender, i.e., incoming LAN segment, and records sender location pair in bridge table.

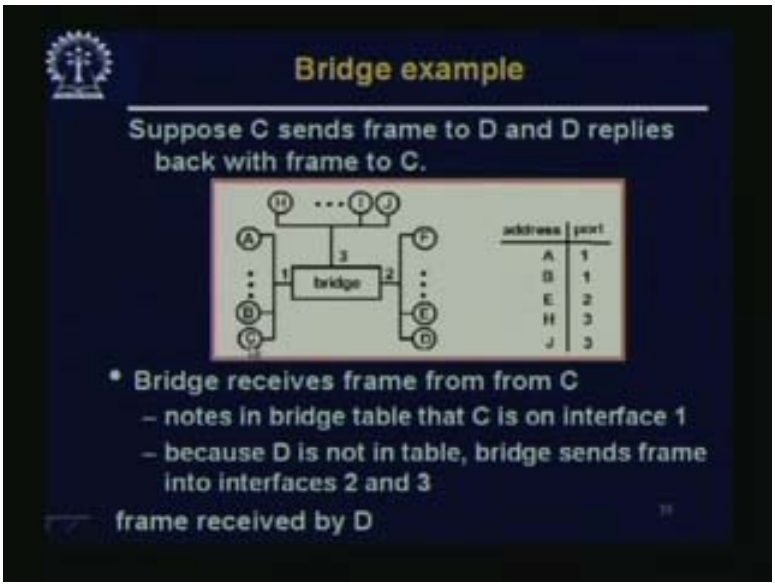
(Refer Slide Time: 38.10)



When a bridge receives a frame, it forms an index bridge table using MAC destination address. If an entry is found for destination and if the destination is on the segment from which the frame had arrived, it drops the frame, because the frame is already in the particular LAN. If an entry is found for destination and if it has to go to some other LAN, it will

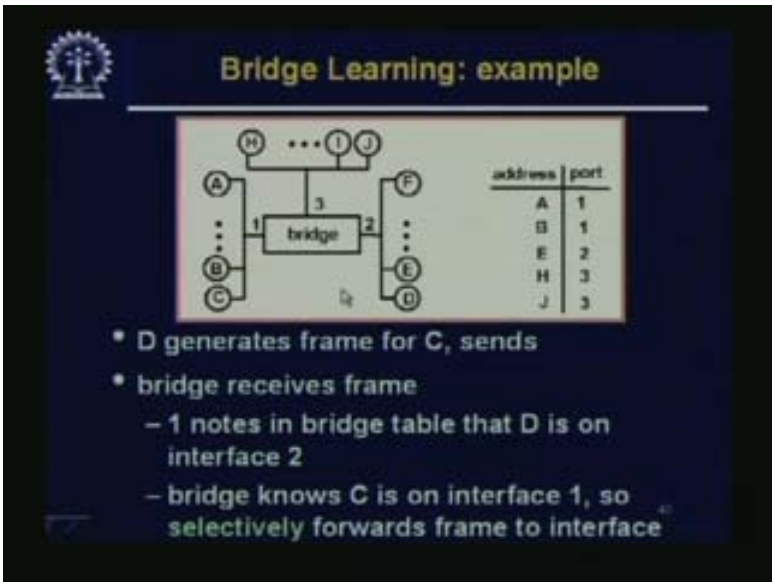
forward it. This is known as selective forwarding. If this packet frame is meant for some other LAN, the bridge will forward it to that particular interface. Sometimes a new machine is connected to the LAN, etc. or the bridge is newly connected and its bridge table may not have been constructed fully and so it may not have an entry for this particular MAC address. In such a case it will flood. Flooding means forwarding the frame to all interfaces except the interface on which the frame arrived. When a particular frame arrives from some interface for some destination MAC address and the bridge does not know to which LAN segment this MAC address belongs, it does not have a corresponding entry in the bridge table. So it will simply flood, i.e., put in a copy of the frame to each of the other interfaces. If a bridge is newly put in a network, in the beginning it will be inefficient as we have already seen, flooding many packets to many segments. But as it slowly learns, it will become more and more efficient.

(Refer Slide Time: 39.58)



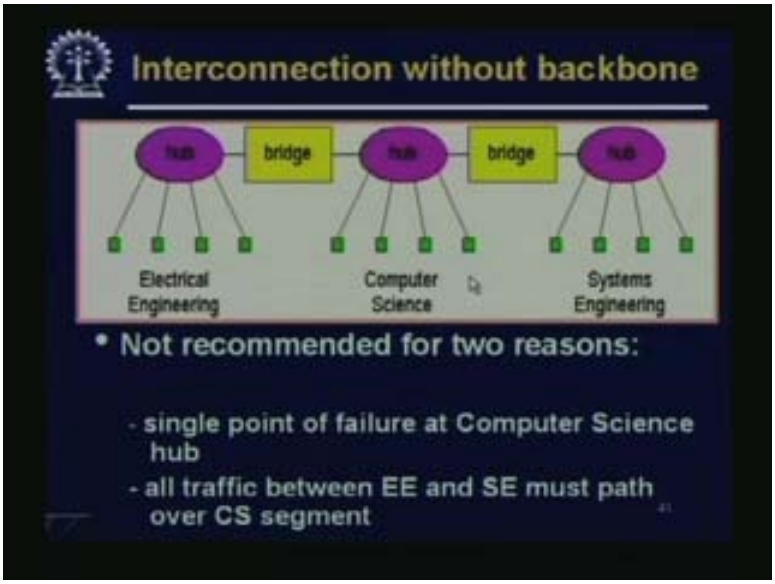
Suppose C sends a frame to D and D replies back with a frame to C and the bridge has this address table and C is on interface 1. Let A and B be with port 1, E in port 2, H and J in port 3. The bridge doesn't know about either C or D. So when the bridge receives a frame from C, it notes in bridge table that C is on interface 1. This table will get updated because C is the sender MAC address, which it will put in its MAC table. Still the bridge does not know where D is and it will send the frames into interfaces 2 and 3 and not to 1, as we have seen earlier. The frame gets copied on to other ports, 2 and 3. In interface 3, D is not present. So the host will ignore that frame in 3. But interface 2 has D in it and so D will receive it and will try to reply back to C.

(Refer Slide Time: 41.26-41.56)



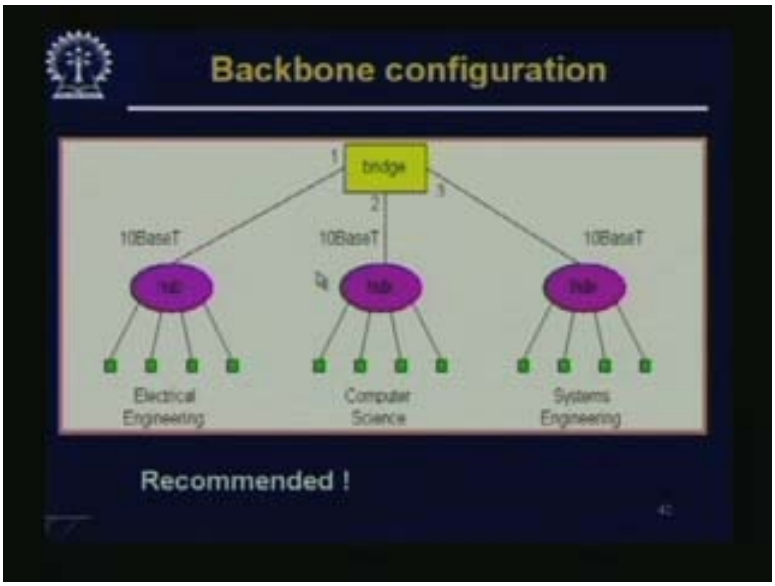
Now D generates a frame for C and bridge receives the frame. One notes in bridge table that D is on the interface 2. Bridge already knows that C is on interface 1. So it selectively sends the frame to interface 1 and does not give to interface 3 any longer.

(Refer Slide Time: 41.57)



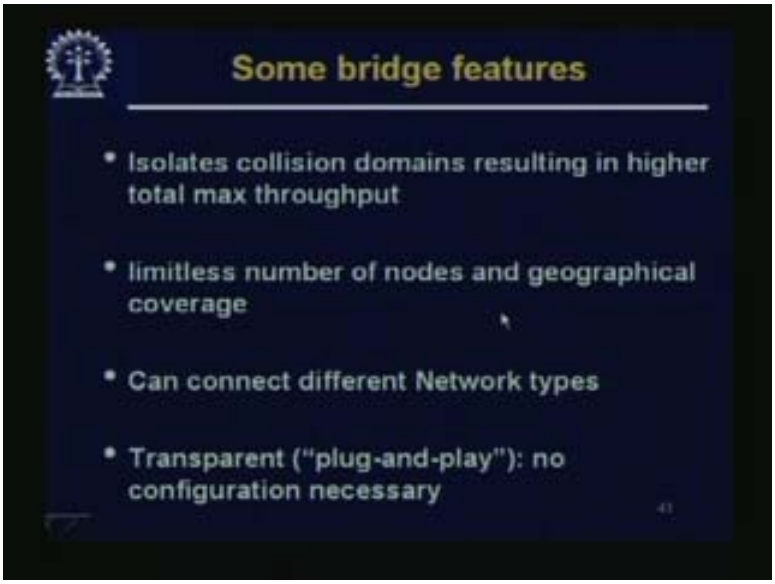
We have LANs and when they get bigger and bigger they can't really exist as 1 single collision domain. So we have to segment it, i.e. break it up into segments and bridge is 1 way to do it. One way of segmenting some of the LANs is shown above. There are three hubs with each hub having a work group. We can connect them through bridges but this is not recommended for two reasons: First of all single point of failure at computer science hub. If this hub goes the other two can't communicate with each other and all traffic between EE (electrical engineering) and SE (system engineering) can't pass through CS, which is not good.

(Refer Slide Time: 43.05)



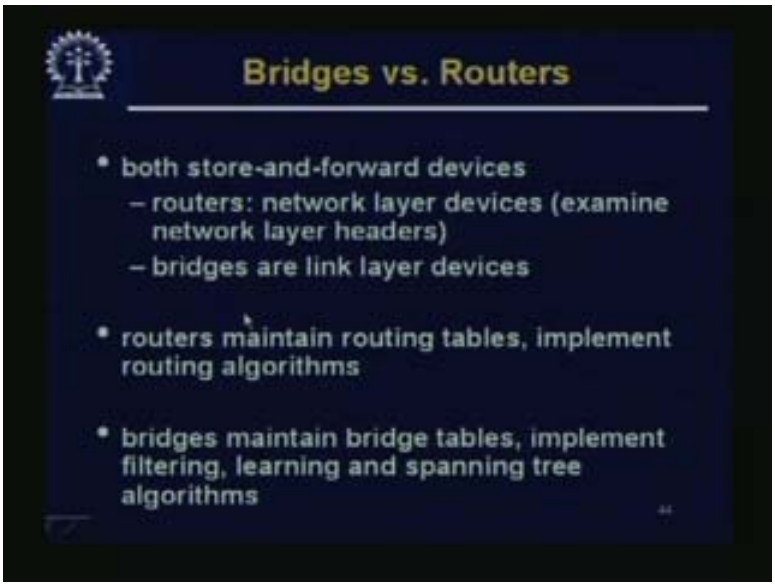
So the recommended configuration would be something as shown above. A bridge or a switch here connects all the hubs. And this bridge or switch acts as the backbone. If EE wants to communicate with SE, it goes through the backbone.

(Refer Slide Time: 43.37)



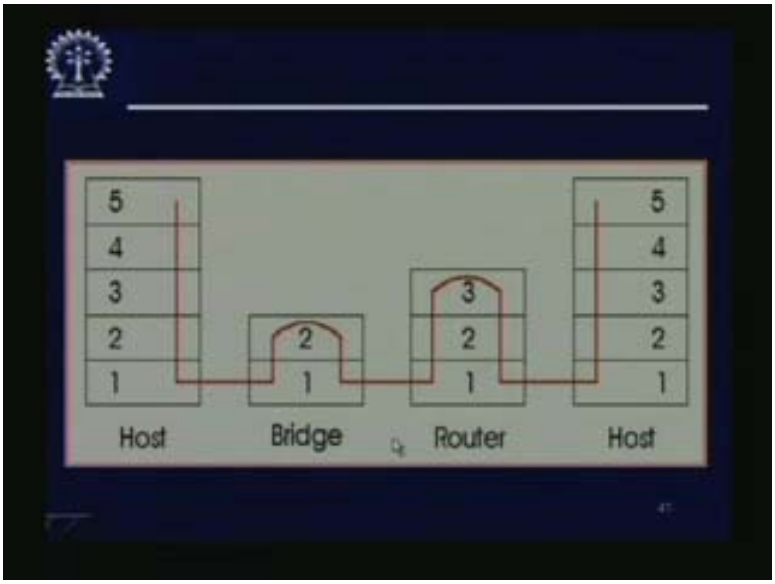
Let's see some of the features of bridges. A bridge has the features similar to a switch. It isolates collision domains resulting in higher total maximum throughput. Because in a collision domain with a lot of broadcast traffic the net throughput of the network will go down. So if you can make it smaller and make the frames to travel from one segment to the other, the overall throughput of the network increases. Also it supports limitless number of nodes and geographical coverage. Bridges can connect different network types. It is transparent (i.e. plug and play) and does "self-learning". So no configuration is necessary for its operation.

(Refer Slide Time: 44.26-46.15)



Now let us compare a bridge with a router. Both are store-and-forward devices. A router is a network layer device (examine network layer headers) and is used for connecting two different networks globally. A bridge is a link layer device and is used for connecting two different networks in local internetworking rather than global internetworking. Routers maintain routing tables and implement routing algorithms. But bridges maintain bridge tables and implement filtering, learning and spanning tree algorithms. Bridges maintain bridge tables consisting of MAC addresses but routers maintain routing table consisting of IP addresses.

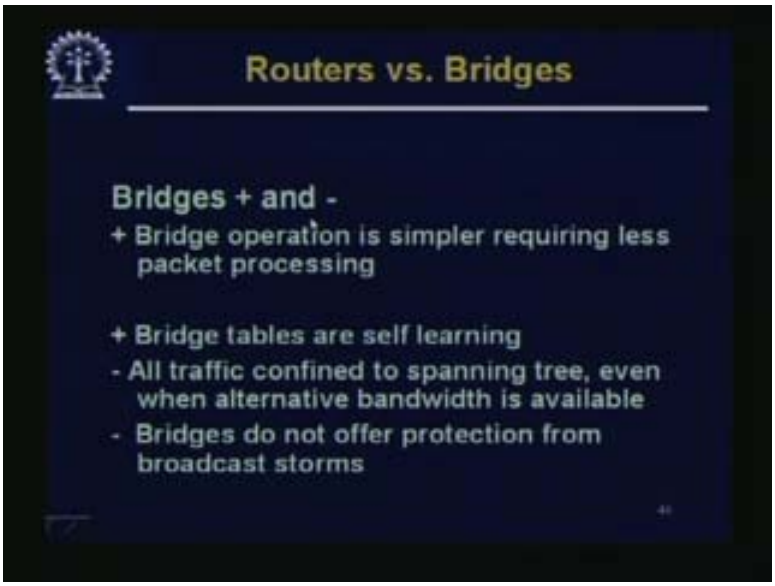
(Refer Slide Time: 46.16)



These are the layers in the protocol stack of the host and from the higher layer, i.e. layer 5 a frame is coming down to 4,3,2,1. 1 is the physical layer and from the physical layer it travels to the bridge. Since the bridge is the layer 2 device, it goes only up to layer 2. Then it encounters a router in the next hop and router will take it up to layer 3, and again bring it

back and then send it to the host. The frame will again go to layer 5. So a bridge is the layer 2 device and router is the layer 3 device.

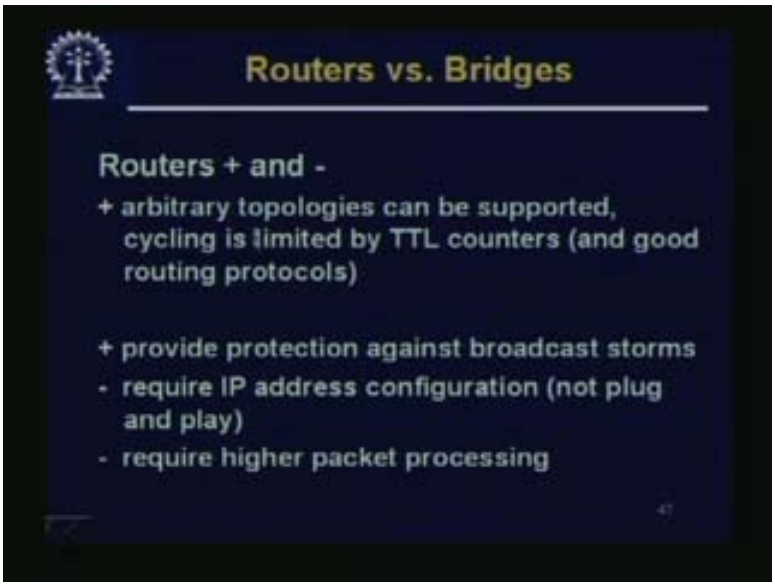
(Refer Slide Time: 47.10)



Let us see the advantages and disadvantages of a bridge. The advantages are:
- bridge operation is simpler requiring less packet processing
- bridge tables are self-learning
- no configuration is necessary and
- all traffic confined to spanning tree even when alternative bandwidth is available

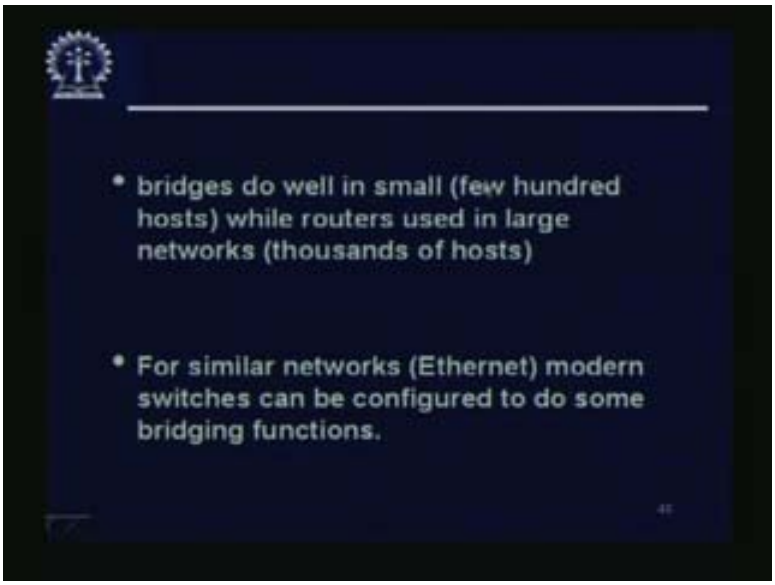
The disadvantages of bridges are, As we disable some of the links while we run the spanning tree algorithm, at a time, only some of the links are used while the rest remain idle. So we are not using the total bandwidth that is available to its fullest and bridges do not offer protection from broadcast storms.

(Refer Slide Time: 48.20)



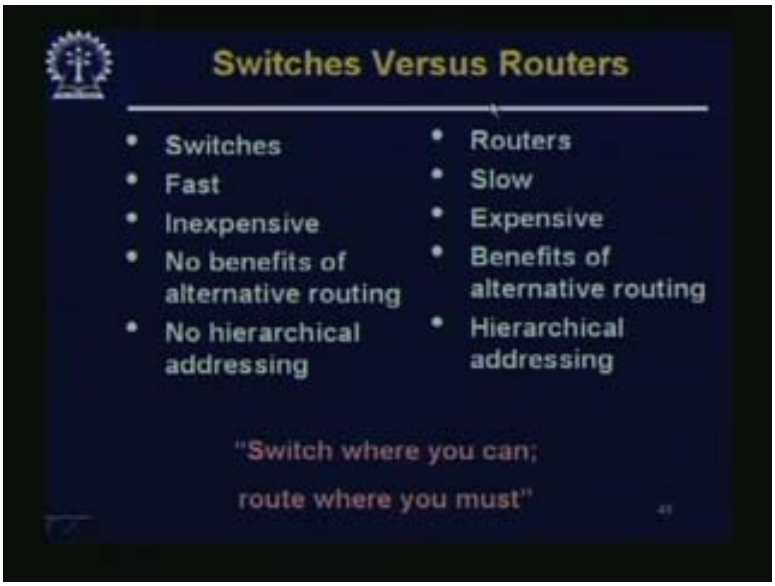
Let us now look into the advantages and disadvantages of routers. The advantages are - arbitrary topologies can be supported. Cycles are supported in bridges, i.e., a frame may go on and on forever. But in the network layer, the packet will have a counter and if a packet starts cycling, the protocol is such that at each hop the counter will be decremented and if some router finds that this count has become 0 it will simply drop the packet. So there is a definite time for a packet to circulate and so it can't circulate indefinitely. The counters used are TTL counters. It provides good routing protocols such as limiting the cycles etc. The network becomes better. The router is capable of providing protection against broadcast storms. The disadvantages are - it requires IP address configuration which means that it is not a plug-and-play device. It requires some manual configuration and higher packet processing. So it is costlier.

(Refer Slide Time: 50.03)



Bridges work well in small networks, i.e. with few hundreds of hosts while routers are used in large networks, i.e. with thousands of hosts. Also for similar networks like Ethernet modems, switches can be configured to do some bridging functions. As we have seen already, whatever functionality is available in the bridge is available in modem switches also. Now let's compare switches with bridges and routers respectively.

(Refer Slide Time: 50.35)



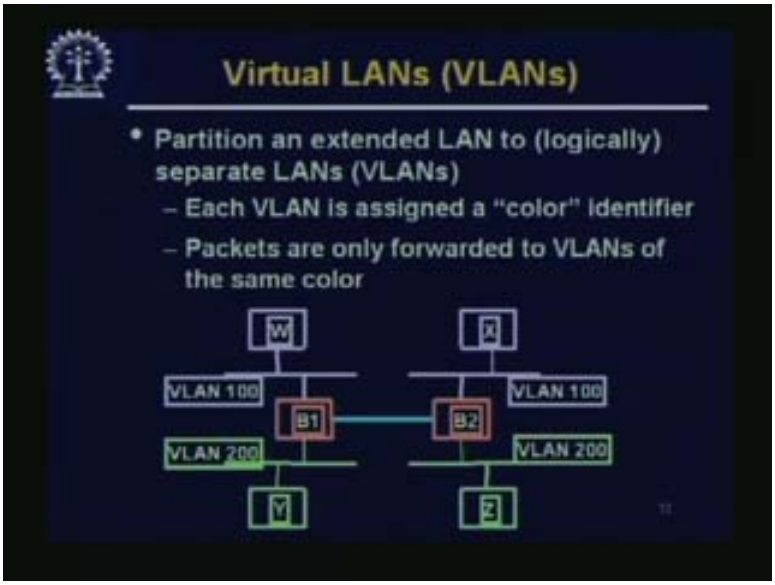
Switches are very fast but routers are slow, i.e., switches are doing just switching so they are very fast whereas routers have to do some computation and so they are slow. Switches are inexpensive but routers are expensive. Switches don't give the benefit of alternative routing whereas benefits of alternative routing are available in routers. There is no hierarchical addressing in bridges, but hierarchical addressing is possible with routers. Hierarchical addressing will be discussed later. When we are connected to the wide area networks, i.e., to the whole wide world, then router is a must because other people can also connect through routers and the routers will talk to each other. But switches can't talk. If you are trying to do local internetworking, a bridge or a switch which now-a-days gives all the bridging functions, may be a good, cheap and efficient alternative.

(Refer Slide Time: 51.57)

Let us finally summarize the comparison between hubs, bridges, switches and routers.

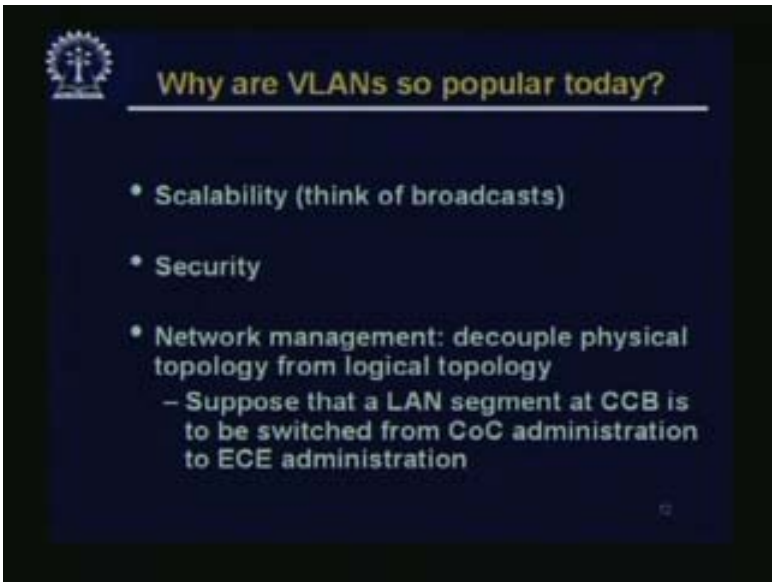
- Traffic isolation - Bridges, routers, switches provide traffic isolation where as it is not possible in hubs. Because a hub is just a shared medium that does not give any isolation at all.
- Plug-and-play - Hubs, switches and bridges are plug-and-play devices. But routers need some configuration so it is not a plug-and-play device.
- Optimal routing - Hubs, bridges and switches do not know about routing. But routers can find the optimal route at any particular point of time.
- Cut through - Cut through means you start transmitting as the bits arrive. A hub can cut through because it is a replacement of a passive shared medium, so whatever bit comes, gets transmitted. So cut through is possible in switches also. But bridges and routers have to wait for the whole frame and then inspect it through some routing table or bridging table so they are not cut through.

(Refer Slide Time: 53.35)



Finally let us see about virtual LANs. It is partition of an extended LAN to logically separate LANs (VLANs). Each VLAN is assigned a color identifier and packets are forwarded only to VLANs of the same color. So we can use a bridge or a switch. The different ports of a switch could be different VLANs. The ports belonging to the same particular VLAN may physically be two different LAN segments. But logically they are in the same VLAN. Suppose in one building, computer science is in three different floors and the same floors are also shared by say, the electrical engineering department. Each floor has a switch. The computer science floors 1, 2, 3 are in same VLAN or they are in one logical group. Electrical engineering in these floors forms another VLAN. This needs manual configuration but this is possible.

(Refer Slide Time: 54.59)



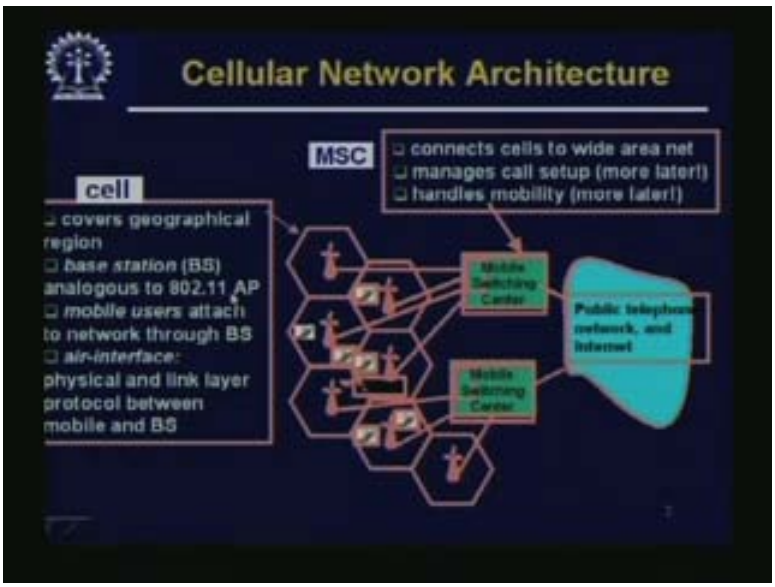
Why are VLANs so popular today? Scalability is possible because broadcasts are now getting limited. Security and network management is better in VLAN. Network management is decoupling physical topology from the logical topology. As we have seen, two different LAN segments could be in same VLAN. For example, a LAN segment at CCB is to be switched from COC administration to ECE administration. We have finished our discussion on local internetworking. Next, we will see another emerging technology, which is becoming very important in the retailing business. Let us see about Wireless Technology in the next lecture. Thank you.

Computer Networks
Prof: Sujoy Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture - 22
Cellular Networks

(Refer Time Slide: 55:52)

We will start our discussion on terrestrial wireless networks. We have already seen 1 kind of wireless communication which is through satellite. It is a microwave repeater. There are 2 very important and rapidly expanding fields in networking. They are terrestrial wireless networking and wireless LAN. We will have 2 lectures on this. The first lecture is on cellular networks and in the next lecture we will talk about wireless LANs and a little of wireless MANs. Today we will discuss about cellular networks.

(Refer Time Slide: 56:52-58:47)



The cell phones have become ubiquitous nowadays. What is a cell? In the cellular network, the network is organized in the form of some cells and each cell covers a geographical region. It has base station (BS) analogous to 802.11 AP. AP stands for Access Point. 802.11 is the wireless LAN technology which will be dealt in the next lecture. There is a base station and it will have an antenna and some transmitters and recivers and they are connected to the backbone through a line. It is a wireless line but usually it would be a fibre optic line. Take this particular base station shown. All the mobile stations or mobile users in the certain geographical location around this base station will communicate with this base station and through this base station to the rest of the network. So mobile users attach to network through BS and air interface is the physical and link layer protocol between mobile and BS. All the base stations are connected to the mobile switching center (MSC). The switching is essentially done here. The MSC connects cells to Wide Area Network.