Communication Networks
Prof. Goutam Das
G.S. Sanyal School of Telecommunication
Indian Institute of Technology, Kharagpur

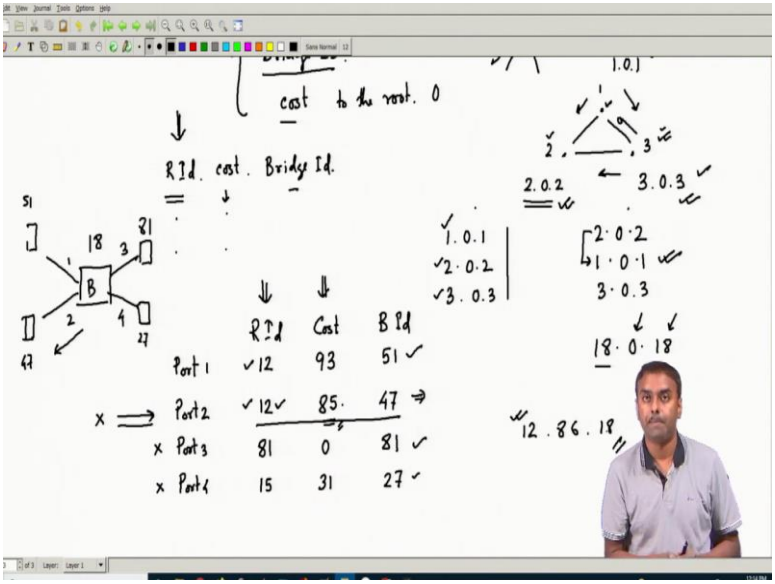
Module - 11
Bridges
Lecture - 53
Distributed Spanning Tree contd

Ok. So, we have been discussing this Spanning Tree algorithm. We have seen how the messages are being constructed and how we can actually take those messages and compare them and then come up with the next phase of messages. So, that is something we started exploring.

So, we will go forward in that direction a little bit more to find out how in a distributed fashion just by exchanging those messages bridges can decide about their spanning tree. In a local fashion in a distributed fashion, but that spanning tree that they will be constructing will be in a collaborative way unique ok. So, that is something we want to see. This protocol was given by Radia Perlman which we have already discussed.

So, so far we have seen this message comparison. Now let us try to see that from some set of messages that we have received. How do we calculate? What should be my designated route and then what should we do with that? How should we construct the next messages?

(Refer Slide Time: 01:40)



So, let us say I have a switch or a bridge that has 4 ports and this bridge has ID 18 ok. So, he has himself his ID is 18 this is port 1 2 3 4. Now what will be happening? He will be receiving some of the messages ok? Let us say in all these messages what he receives I will list that. It is a hypothetical case I am just giving examples of port 1, port 2, port 3, and port 4.

Of course, everywhere I will be receiving three things the message has three particular things that are defined root ID means cost to the root, and then bridge ID ok. So, first is this root ID ok then cost to the root, and then bridge ID who is transmitting it.

Let's say port 1 of course, will be connected to some other bridge. So, that bridge is telling that the root ID he has so far explored is 12 cost to that root is 93; that means, 93 hops it is a very big network ok 93 hops are required to reach over there, and his bridge ID that neighboring bridge Id is 51.

Similarly, this second one also has explored that 12 should be the root ID 85 is the cost to that root and 47 is his bridge ID. So, the second port is 47 bridge this is 51. For the third port, he says 81 is this thing's root ID cost which is 0 because he has not explored anything so far. He still thinks that he is the root and therefore, his ID is 81. So, that only he thinks as root.

The other one also has explored and he thinks that 15 is the root ID 31 is the cost to reach that root and 27 is his ID. So, the third one is connected to Bridge 81 and the fourth one is connected to Bridge 27 ok. So, these are the 4 messages he is receiving. Now he will compare.

Comparison as you there is a priority. So, first I will be comparing the root IDs if there is a tie then I go to the next one. So, root IDs which are the lowest one two are the lowest. So, these two are already discarded these two messages are of no importance. Because if I go the root Id will be higher 81 is higher than 12 15 is higher than 12. So, I know these two mean these two have lower root I d.

So, they can qualify for root 12 ok if locally whatever copy I have I do not know anything less than 12 to be root. If that is the case then probably that will be my still designated root let us say I have something which is more than 12. So, my node ID is 18 suppose I have not learned anything. So, I still have this message 18 0 18; that means, I declare myself to be root and that is my ID and the cost is 0.

So, if this is the case if I compare my message with this guy's message it is still low right. So, therefore, between port 1 and port 2, somebody must be on the path. Now I will see the cost I can see that this guy requires lesser cost to reach the root. So, therefore, if I go via him I will be taking less amount of paths or I have to traverse less amount of hops to reach the root. So, therefore, I will be taking him.

If it was even tied over here then I could have checked the bridge I'd ok. So, that also is the third tiebreaker ok? So, over here I can immediately decide that this must be the port that I should target for. So, therefore, port 2 must be which is towards the root. Now if port 2 is towards root. How do I construct my new messages? So, now, what is the next information that I know?

I know I have already decided that locally now my decision for root is 12, how do I reach that? I reach that via port 2. Port 2 has already reported the cost to be 85. If now I have to tell to my neighbors what will be the cost to that root I have to add one more count. Because he has to first reach me and then from means he has to reach me and from me I go to the next node to root is 85.

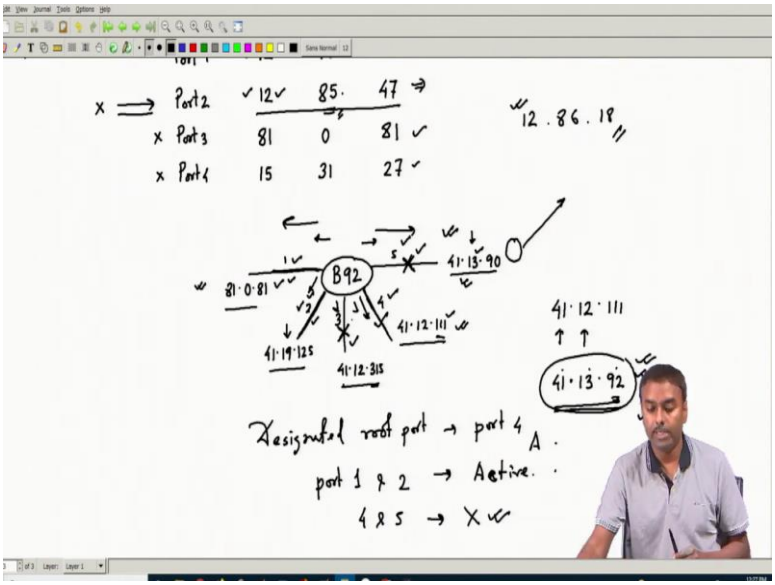
So, I have to first reach the next node. So, that is 1 hop and he has reported 85. So, it should be 86. And how do you reach that? Via me, if I am telling others that this is the root you can reach via me through 86 hop count that should be via me. So, that should be 18 which should be the new message constructed. This should be my new message constructed and where do I forward this?

I forward it not to port 2 because port 2 is port 2 already knows. Port 2 has a better message as you can see 12 points 85 points 46 and I have a message of 12 points, 86 points, 18. So, he has a better message. So, I do not have to forward him. I rather get a packet and forward it to him ok? I do not have to forward this control message to him because he knows already a better direction towards reaching the root.

So, therefore, I will not forward it to port 2 I will forward it to all other ports wherever compared to their message I have a better message ok. So, those are the places where I will be trying to forward these things ok? Let us try to take another nicer example and then try to see exactly after deciding what is the better root and what is the cost of that root after deciding that one how does he decide which should be the designated port and which should be the blocked port?

Because for the spanning tree, I need to block some of the ports I need to decide that ok this is the port that should be taken out from the tree.

(Refer Slide Time: 09:01)



So, let us try to decide that part. So, for that, we will take a particular example. So, what is that example? So, let us take that example. Let us say I have a bridge which is B and the address is 92. It is connected with 4 ports ok. So, port 1 then 2 4, 5 ports; 3 5, and 5 ok.

The messages that I am receiving from them are something like this. 81 dot 0 81. So, he thinks that the next bridge is 81 and he thinks that he is the root. So, that is why 0 cost is required if you go via him to reach the root and his ID is 81. This guy has learned a little bit extra he thinks 41 is the root 19 hops are required if you go via him and his ID is 1 25.

3 knows 41 is the root and if you wish to reach via him 12 hops are required and 315 is his Id. The next one knows 41 dot 12 dot 111 and this is 41 dot 13 dot 90 ok. So, that is that is the overall thing. These are the messages he will be receiving. After receiving all these messages now he has to decide.

So, now let us try to compare them. What is the lowest root ID? This is at a particular middle stage of this algorithm when a lot of messages have already been exchanged few of them have started learning what should be the root. So, probably in the entire network 41 is the lowest root Id let us say ok.

Then all these other ports whichever bridges are connected have already learned this guy probably has not learned yet he is still thinking for some reason maybe he has started late or whatever it is he is still thinking he must be the root, but do not worry because of this 1 stage message passing he will be immediately in the next stage he will be knowing because this guy will be giving some message that will immediately have the information and he will learn it.

So, basically, this learning just takes place in this fashion ok. Now if you see all these things. So, what you can see from all of them we can already see 41 is probably the root because everybody has 41 and in 41 all ports 2, 3, 4, and 5 are tied. So, 41 must be the root. Now let us try to see cost-wise who is least costly. This guy gets 13 12 12 and 19.

So, of course, 12 must be the lowest one. So, 12; that is the lowest one. Now among them what is the. Now both of them are tied; so, root ID is tied among nodes linked this ports 3 and 4 and even cost is tied. So, whom should I choose? Now with respect to the

bridge I d. So, this is the last tiebreaker. So, I see that this has a lower bridge I d. So, I will declare 1 1 1 must be the 1 ok.

So, this message is winning so; that means, that port 4 is the port through which I should reach my root ok. So, that must be the port I should target whoever's packet means I should say that this is the way towards root via port 4 and that is what I should report to all others. So, what do I tell to them?

I know he has already reported this one. So, to reach him one more hop I require because this is immediate neighbors these things. So, my message should be 41 dots 13 dots 92 because that is my bridge ID. This is the new message that I will be constructing. Now among these new messages, I have to see this new message if I transmit where should I mean who will be taking that?

So, if you carefully see this. Now this particular guy ok this bridge has a message who has earlier transmitted a message 41 dot 13 dot 90 ok I am giving him 41 dot 13 dot 92. Definitely, he will not be taking that right. So, he will he will never take that right. So, that is one thing one understanding I will be having because he knows a better root. So, that is something he will not be doing.

Now, let us try to see what is happening. If this is 41 dot 13 dot 92 I have decided from myself that this is my message. Now let us try to see port 5 and port 4 ok. Port 4, what is happening? Port 4 is already the root ok. So, that is that is the targeted root direction. So, that must be the root direction this is my root direction ok? Think about these two; port 1 and port 2.

They have a message that already means comparison-wise much bigger than mine. So, I will be winning so, therefore, these two become my designated ports because those two guys must learn from me. Right now whatever information they have? They must learn from me. So, therefore, these two I will still be as if they can always according to their current understanding they can still go via me and get a better deal on reaching the root.

So, therefore, if these two links I will keep open they must be according to my current decision they must be the designated link. So, that they come via me and go over to the root. Now think about this particular link and this particular link. If you see they have a better deal in some other direction ok, they have a better deal via some other direction.

So, therefore, I will actually block these 2 links. So, this is how I design my network. So, what I will be doing? I will be saying that these two ports are no longer part of the according to my current understanding, of course, this understanding might change. According to my current understanding, these two ports must be taken out to facilitate the spanning tree otherwise there will be a loop.

Because they already have if you think about this neighbouring node they already have a means path to reach to the root which has a better configuration than if they go via me. So, therefore, they should not go via me. So, this is the thing link that I should discard because if I keep that he will be taking that other root as well as my root. So, therefore, that is the link I should discard. I will be discarding this 1 I will be discarding this 1 this will go to the root.

So, I will keep these two. So, what has happened? Now after all these things my designated root port is port 4. So, via port 4 I know that I can reach to the root that must be activated. So, this is active. Now ports 1 and 2 that is part of the spanning tree because they must reach according to my current decision current understanding they must reach to root via me. They have this as the best path all other paths they know that is not better than this one.

So, therefore, they will be coming via this. So, those 2 port I should keep them active Ports 1 and 2 must be also active sorry. And port 4 and 5 I actually take them out from the graph. So, those are the candidates that should be taken out to construct my spanning tree. Because of obvious reasons, they have some other link to the root which is already lower cost.

So, therefore, this must be redundant if I keep that that will be constructing that loop. They will have alternate roots also which is one of them is costlier than the other one. So, therefore, if I take out that link I can say safely overall in the network my neighbours are getting a better root and they do not need me and that is why I am taking out those things. Like this, every node will be deciding which link should be taken out.

As you can see because they are linked via these messages they will always decide the same thing. Those two nodes also will know that ok this link is because the message they will be getting will be immediately knowing it will be consistent they will know that

ok via him if this guy gets a message via 92 I should not reach the root I have a better way to reach the root.

So, they will have consistent learning from neighbor to neighbor to neighbor and they will construct the spanning tree by passing messages one after another. So, this will be happening. This is guaranteed to happen as you can see already and this is how they will do. So, basically whichever I keep active what does this mean; that means, on those particular ports as we have already decided in the spanning tree if I keep some link or some LAN active.

That means on those ports I will be forwarding packets or I will be receiving packets from there if some packets are coming on there. So, I will be doing that plus I will keep on learning on those ports. But if I discard like ports 4 and 5 I will not be receiving any packet I will not be forwarding any packet. So, it is the actual data packet I am talking about.

And I will not be learning on those ports if any packets are coming on those ports I will not learn that ok these nodes are connected on those ports I will not be doing that. But remember, my protocol still continues; that means, the spanning tree protocol which is the control part of the protocol that continues in all the ports.

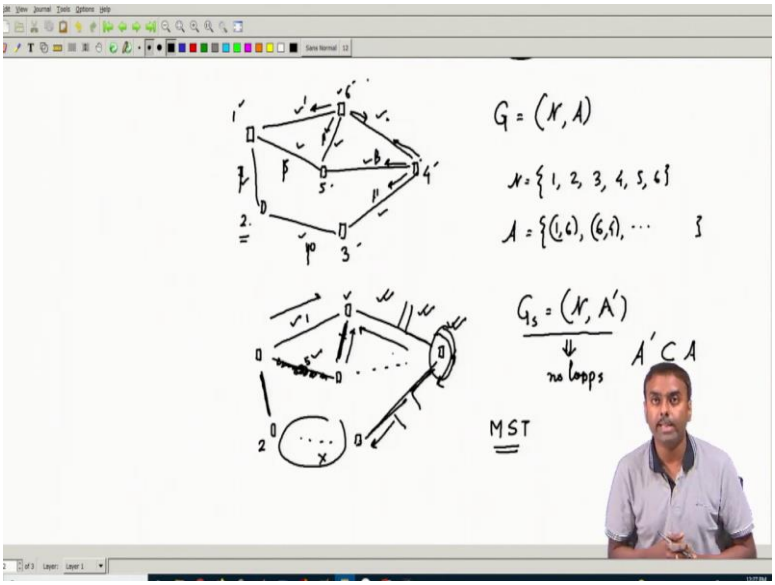
So, every port I will be still sending whatever message I have constructed that I will be sending to all ports. So, control messages I will keep on sending and control messages I will be receiving for spanning tree purposes because that helps me to keep on going on the spanning tree.

So, these control messages I will keep on transmitting. The only thing is that I will no longer whenever I decide that some port. I deactivate I will not be taking any data packet from that port I will not be forwarding any data packet and I will not be enabling any learning from those data packets.

So, that is exactly what we will take out, but in all other ports that I have decided to keep active, I will keep on doing my all other functionality data forwarding, data receiving and then learning from the data. So, that is how together the spanning tree protocol and the data forwarding protocol keeps on going.

So, with this, after sometimes it will converge, this spanning tree protocol will converge and it will decide upon the particular spanning tree that is there.

(Refer Slide Time: 21:37)



Now, the good part of this because you will be keep on running that spanning tree algorithm. So, a good part of this is that suppose some link or some LAN or some bridge is failing, immediately they will detect that because they will not receive any packet from there that neighbor they will discard.

So, they will not because they will not be getting any transmission from those nodes. So, they will reconstruct their messages and they will again run the spanning tree and they will converge to another spanning tree that connects everybody. So, that is the beauty of it. So, it is a very self-healing kind of network where if any failure happens they again learn the whole thing from scratch in a distributed fashion.

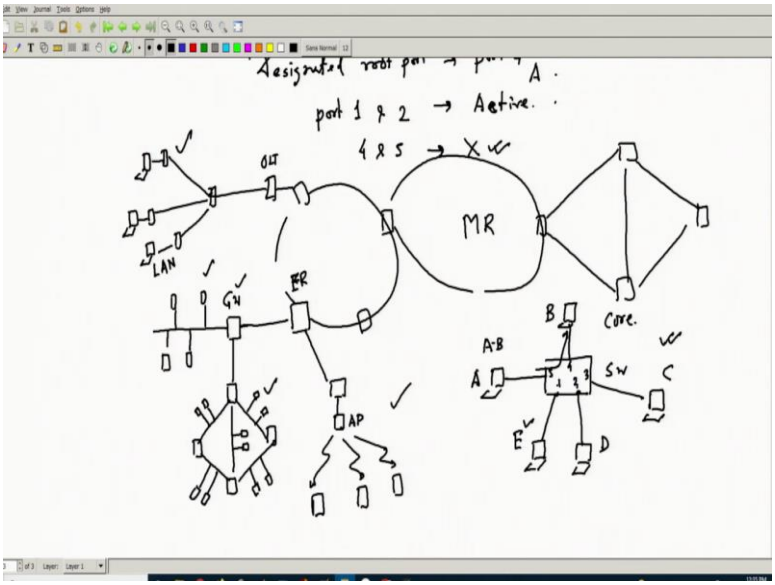
They just keep on exchanging messages and they learn the whole thing they again construct a tree and through that tree, the packet forwarding goes on learning goes on and bridges function very nicely. So, this is the protocol that has been devised as you can see so nicely it can actually facilitate the whole operation. Not only that it also facilitates the operation when there are failures.

There are some LAN failures and some bridge failures; whatever happens, the other bridges immediately learn for themselves and then they construct the new spanning tree

and then they function operating again according to that. So, this means this has been a very important protocol for bridge operation and this has been in place to date. So, with these things if we summarize what happens to the networking now.

So, if you now try to see we have discussed a lot of access level protocols. So, how they are sitting together.

(Refer Slide Time: 23:40)



So, what will be generally happening? So, you might have some campus LAN where multiple stations are connected. Generally, what will be happening later on is that they might have some gateway oh that is called the IP router. So, that will be the layer 3 protocol included. So, a gateway will connect it to the internet or other parts of the network.

So, like this, there might be the same gateway that might have multiple such things it might even have some multiple bridges, which are interconnected among themselves. And those bridges might have their own machines that might happen like this they all get connected to the gateway. Gateway goes to the edge router probably and then from this edge router a particular. So, this is LAN single LAN this is a bridged LAN.

So, multiple LANs are connected together; they all get connected to gateway the this is where the layer 3 switching will be happening or routing will be happening. So, like this, you can actually connect multiple things not only that from the edge router, there might

be another gateway; over there might be an access point wireless access point which is connected from there it is all wireless.

So, all mobile stations can be connected. So, like this multiple LANs can be connected to the edge router edge router might construct the edge network probably this might be a ring with multiple edge routers with multiple other LANs. So, like this, the network gets built up. So, from there edge router there will be probably a metro core router and then you can have a bigger ring which is the metro ring from there the core network might be the core edge.

From there the core edge of the mesh network might start this might be completely a circuit switch network or an optical network. So, this is the core network core it might be national backbone it might be regional backbone it might be international backbone. So, all kinds of things might be happening. So, this is how the network gets built up even over here you might have an OLT you can have PON. So, these are the o n us and then the machines are connected that also might happen.

So, all kinds of LAN solutions might be there sorry all kinds of access solutions might be there they all might coexist in the same network that is what I am trying to say over here whatever we have done we have talked about this, and we have talked about this we have talked about this single LAN we have talked about also multi LAN. So, all these things might coexist and they might coexist with the help of some layer 3 rooter.

So, now if we have to go beyond this we need to understand the layer 3 protocol part of protocol. So, that is what we should be starting next. But before starting that I just want to finish this with a single one so, far we have been discussing this CSMACD kind of or Ethernet kind of LAN ok? There is also something called switched Ethernet what is switched Ethernet?

So, over there what do we do these bridges? Now we can call them switch it is having the same functionality, but what means how we will differentiate them is that we will not be connecting any collision domain or any CSMA CA domain basically all these ports will be directly connected to a machine. So, every port of switch will be connected and these are all learning switches every port there will be multiple ports and you do not have any collision domains. So, everybody forwards the packet and then switches and decides where to go.

Once the switch learns it exactly learns whom to forward the packet. So, basically suppose the switch has let us say 5 ports; that 1, 2, 3, 4, 5 ports. Now if I designate them as A, B, C, D, E for this one. So, the switch will start learning that port 1 has E port 2. So, if this is 1 2 this is 3 4 5 they will start learning which port has which particular station.

And then suppose I send A to B after he has learned he will be just doing this switching. So, the entire broadcast domain was taken out from there and switched to Ethernet operating in this fashion. So, there is no collision there will be a hundred percent utilization and you do all you do because of the learning bridges you do not forward anybody's packet to anybody else it will be all designated packet forwarding. So, that has a huge security also added to it.

All our Ethernet in the lab that you will be using or any other places in the institute you are using these days are mostly the switched Ethernet they no longer go via CSMACD. So, the entire CSMACD we have learned the collision domain collision avoidance, and all those things are mostly nonoperational these days. CSMA CIs wireless access they do it, but for Ethernet you actually connect everybody via either RJ 45 or your optical fiber link 1 GBPS link directly to the switch.

And then it is a switched Ethernet. So, there is absolutely no broadcasting no nobody actually does any kind of packet forwarding to other ports no collision domain no collision avoidance no CSMA nothing. So, with this, we finish our discussion of the underlying layer 2 protocol.

We will cover our discussion or continue our discussion on layer 3 and layer 4. So, that we can see the whole end-to-end perspective of the network and how it operates taking layer 2 into the picture knowing that the DLL layer is at the means second bottom or second last layer, how does this upper layer operate on top of them make the networking happening from end to end. So, this is something that will be discussed next.

Thank you.