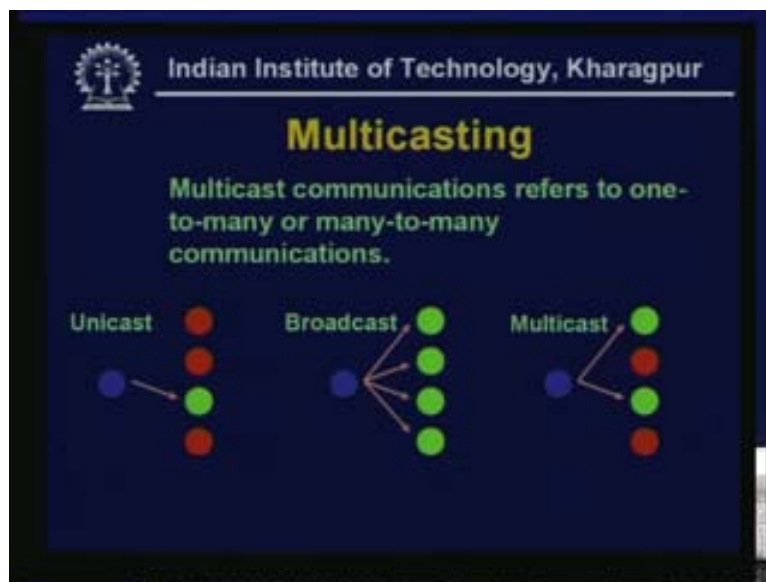


Computer Networks
Prof. S. Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture - 32
IP Multicasting

Good day. Today's topic is IP Multicasting. Till now, we have seen the three modes of operation: One is unicast where one sender is sending to one receiver. One is broadcast where one sender is sending to all the receivers that means all the nodes in the network and multicasting is when you want to send it to a group of hosts but not all the hosts. So, IP multicasting is the topic for today.

(Refer Slide Time: 01:31- 01:53)



Multicast communications refers to One-to-many and many-to-many communications. For example, this is unicast when the source is one and the destination is one, broadcast is when source is one and destination is all and multicast is when destination are a few.

(Refer Slide Time: 01:53- 02:14)



- IP multicasting refers to the implementation of multicast communication in the internet.
- Individual hosts are configured as members of different multicast groups.
- Multicasting is not connection-oriented.
- An IP multicast group is identified by class D address.

These are the general parameters. One particular user may be member of different multicast groups but for one particular multicast group there will be few members in the network and it has to reach those and not others. Other thing to understand is that multicasting is not connection-oriented that means all the packets are sent. It is packet by packet it is not that from the source multiple channels are prairie setup or anything like that.

(Refer Slide Time: 02:46- 03:15)



They are identified by class D address which is for multicast. The class D address is seen in the fashion that the beginning four bits are 1110. So the initial value is 224 point something and these 28 bits. This is how by looking at an address you can see that this is the multicast address.

(Refer Slide Time: 03:15- 03:26)



There are many applications like news, sports, stock and weather updates. Let us take the example of stock updates. Now, not everybody would be interested in stock updates, only some group of people would be interested in stock updates. Again, it may be such that one group of stock is of interest to one group of people, another group of stock to another

group of people and so these would be different multicast groups and the news feed should reach these people. Then multicasting may be applied in distance learning.

(Refer Slide Time: 03:49 - 04:17)



When some learning material is distributed to distance learners and just specific group of learners, configuration, routing updates, service location may be the areas where multicast may be applied. PointCast-type push applications where push means when the actual source of information finally on its own sends it to the group of people. For example, stock quotes may be pushed.

(Refer Slide Time: 04:28 - 04:52)



Teleconferencing, audio, video, shared whiteboard, text editor etc is an interesting and important application of multicasting. That means you may like to have a video conferencing amongst a group of people so this same video stream should reach the entire group of people.

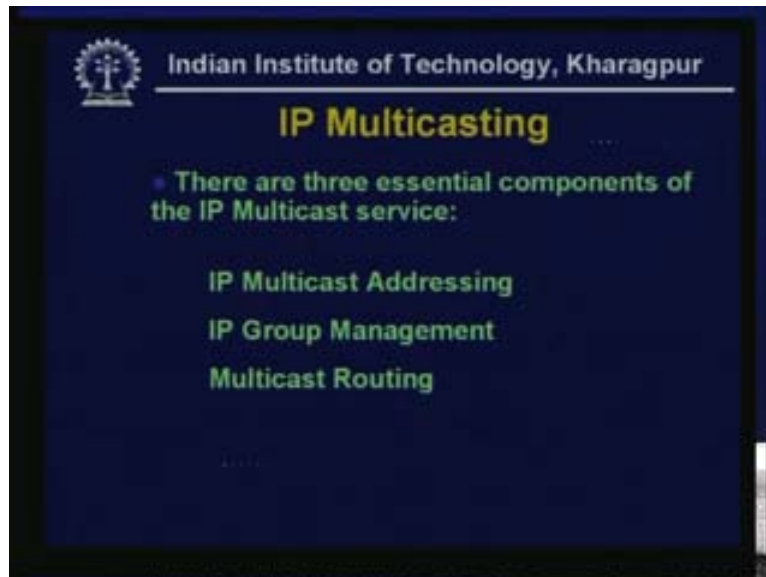
(Refer Slide Time: 04:52 – 05:18)



- Distributed interactive gaming or simulations, some people are participating in some game in a distributed fashion.
- Email distribution lists.
- Content distribution; software distribution.
- Web cache updates
- Database replication.

Multicasting has very large number of applications. But the trouble is, multicasting is a little complex. The technology is not so simple and the fact is there are most of the routers which are in operation today are not configured for multicasting in a proper manner because it takes a toll on the routers capabilities. So we will come to see what a multicast routing is all about.

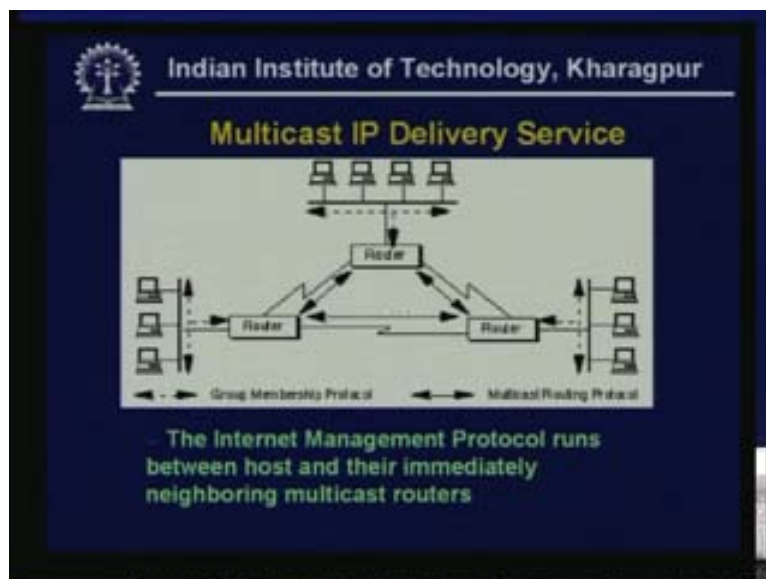
(Refer Slide Time: 05:42 - 05:59)



There are three essential components of IP multicast service:

- IP multicast addressing is, how you address.
- IP group management.
- Multicast routing.

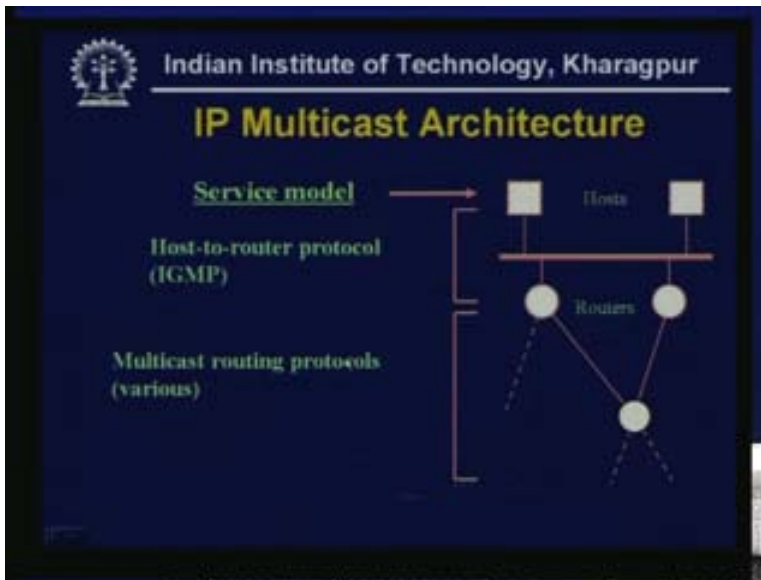
(Refer Slide Time – 06:00- 07:13)



If you look at this diagram, suppose you have these three routers and three networks connected to these three routers respectively. Suppose, you take any of these routers and that is connected to its own group of machines and some of these machines would be the members of a multicast group. Of course, new machines can come in and new machine

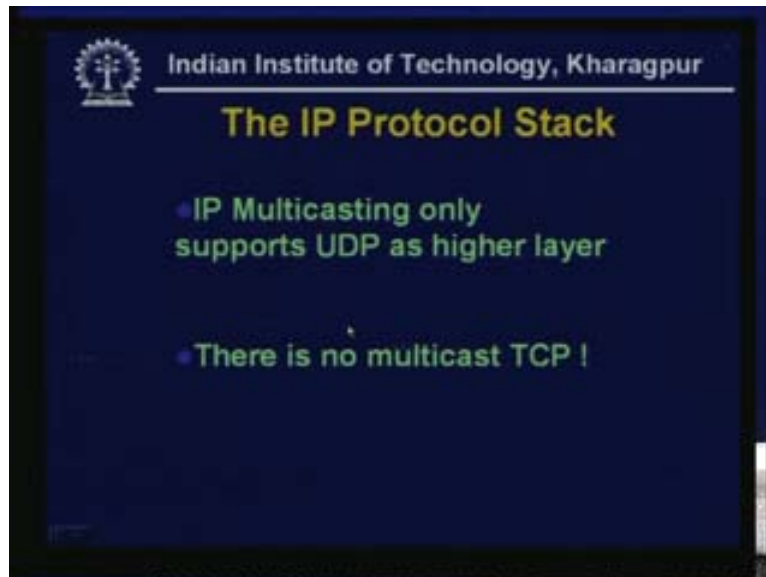
can actually decide to join the multicast group and some of the old group members may choose to leave a particular multicast group. So there is a group membership protocol which goes on between the router and the different machines connected to the network. Then, amongst the routers there is question of multicast routing. So this Internet Group Management Protocol (IGMP) runs between host and their immediately neighboring multicast routers. And within the routers we have the multicast routing protocol running.

(Refer Slide Time: 07:13 - 07:41)



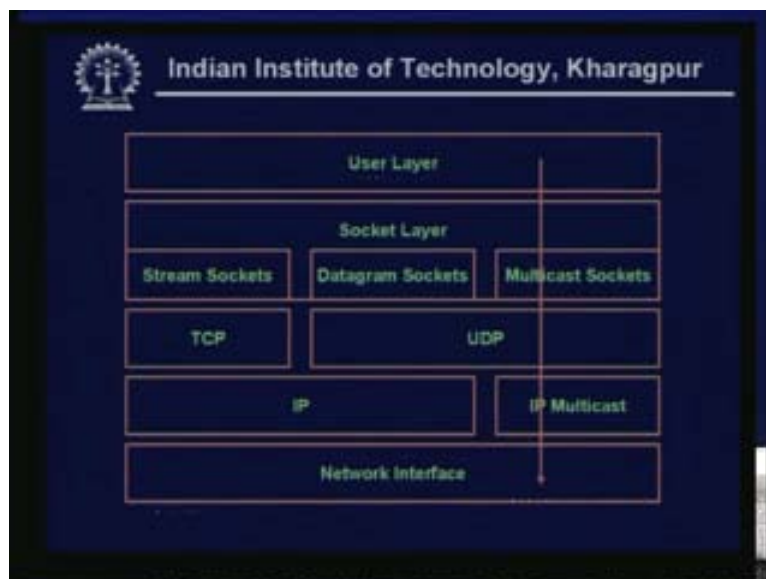
This is another picture showing the same thing. This is the service model, suppose, these are the hosts and host to router protocol which is known as the Internet Group Management Protocol (IGMP). And then amongst the routers there is multicast routing protocol and there are various types of multicast routing protocol, we will just discuss a few.

(Refer Slide Time: 07:41 – 08:07)



- IP multicasting only supports UDP as higher layer.
- There is no multicast TCP. UDP is a connectionless datagram oriented protocol and TCP is connection-oriented. Since, IP multicasting is essentially connectionless that is why it chooses UDP as the transport layer protocol.

(Refer Slide Time: 08:07 - 09:13)



If you look at the details of this part of the protocol stack here we have the network interface, IP and IP multicast layers. The IP part of this network layer takes part in the normal routing protocol whereas IP multicast part takes care of the multicasting routing protocol. Then above this in the TCP IP stack we have the TCP protocol and the UDP

protocol. So, for TCP we use the stream sockets whereas for UDP we use the datagram sockets as well as multicast sockets. So, multicast sockets also use UDP. This is the socket layer and above this we have the user layer. So that is the application layer which uses these multicast sockets and uses UDP to send multicast messages which are routed by the multicast supporting routers.

(Refer Slide Time: 09:13 – 09:51)



IP multicast works as follows:

- Multicast groups are identified by IP addresses in the range 224.0.0.0 to 239.255.255.255. These are the class D addresses.
- Every host (more precisely every network interface card) can join or leave multicast group dynamically.
- At present the way it has been done has no access control. So, if there is a multicast group which requires access control then this has to be implemented in the application layer. As the protocol stands today this has not been included. One of the reasons is that IP multicasting in actual practice constitutes a very small amount of traffic compared to its potential true multicasting. Later on let us see what is true multicasting and simulated multicasting. But actual true multicasting traffic is really small compared to its potential mainly because most of the routers may not support, they are not more precisely configured to support multicasting because of the cost involved.

(Refer Slide Time: 10:46 – 11:06)



Since there is no access control every IP datagram sent to a multicast group is transmitted to all members of the group.

There is no security, no floor control.

Moreover since it uses UDP, IP multicast service is essentially unreliable.

(Refer Slide Time: 11:06 – 11:46)

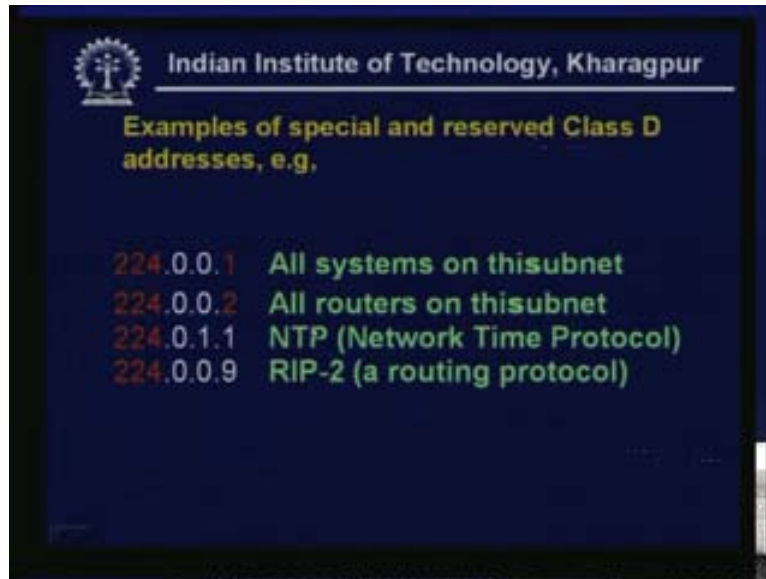


More detail about the multicast addresses:

- The range of addresses between 224.0.0.0 and 224.0.0.255 means the last byte for the first range inclusive is reserved for the use of routing protocols and other low level topology discovery or maintenance protocols.

- Multicast routers should not forward any multicast datagram with destination address in this range. So they are reserved addresses and other addresses can be distributed to different multicast routes.

(Refer Slide Time: 11:46 - 12:21)



Examples of special reserved class D address:

- 224.0.0.1 really means all systems on this subnet.
- 224.0.0.2 means all routers on this subnet.
- 224.0.1.1 is for NTP (Network Time Protocol) used for synchronizing machines.
- 224.0.0.9 is for RIP-2 (a routing protocol).

So these are some special addresses and there are others.

(Refer Slide Time: 12:21 - 12:28)

Indian Institute of Technology, Kharagpur

Multicast Address Translation

- In Ethernet MAC addresses, a multicast address is identified by setting the lowest bit of the "most left byte"

1					
---	--	--	--	--	--

Not all Ethernet cards can filter multicast addresses in hardware -

Then: Filtering is done in software by device driver.

Now there is a question of multicast address translation. You remember what happens in the case of unicast is, from the IP address, for transmitting packets in the local network we need to go down to the data link layer and we need to find out the hardware address. Let us say if we are using Ethernet then we need to find out the Ethernet or MAC address and then data is actually sent as an Ethernet frame so the Ethernet Address is put over there. Now, that is the case when we are handling unicast. Now, what happens in multicast? For this particular IP address it is actually representing a particular multicast group and there will be a number of machines in that group. How do you handle it in the Ethernet level?

(Refer Slide Time: 13:23 - 14:19)

Indian Institute of Technology, Kharagpur

Multicast Address Translation

- In Ethernet MAC addresses, a multicast address is identified by setting the lowest bit of the "most left byte"

1					
---	--	--	--	--	--

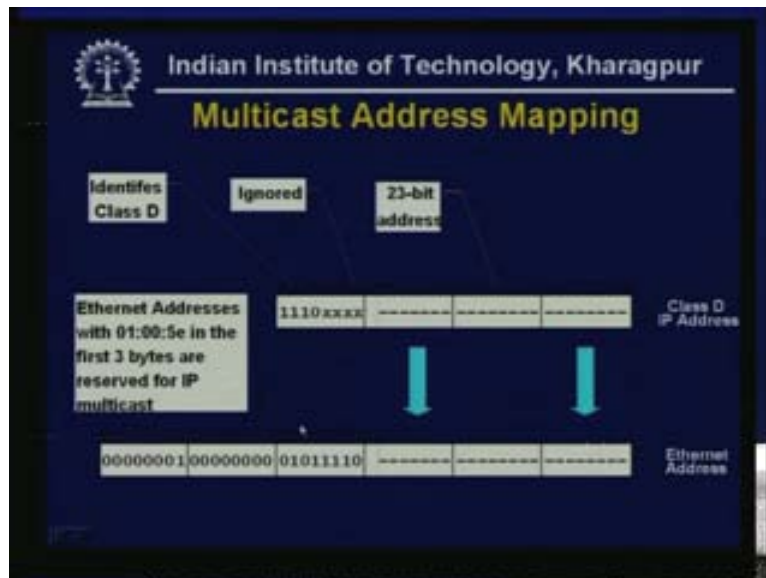
Not all Ethernet cards can filter multicast addresses in hardware -

Then: Filtering is done in software by device driver.

- In Ethernet Mac addresses a multicast address is identified by setting the lowest bit of the most left byte. That is this byte. Suppose you want 1, 2, 3, 4, 5, 6, if you remember, Ethernet address is 6 bytes long, now, of the first byte the most significant byte if you want and the last bit of that is set to 1 in Ethernet Mac addresses to indicate that this is the multicast address.

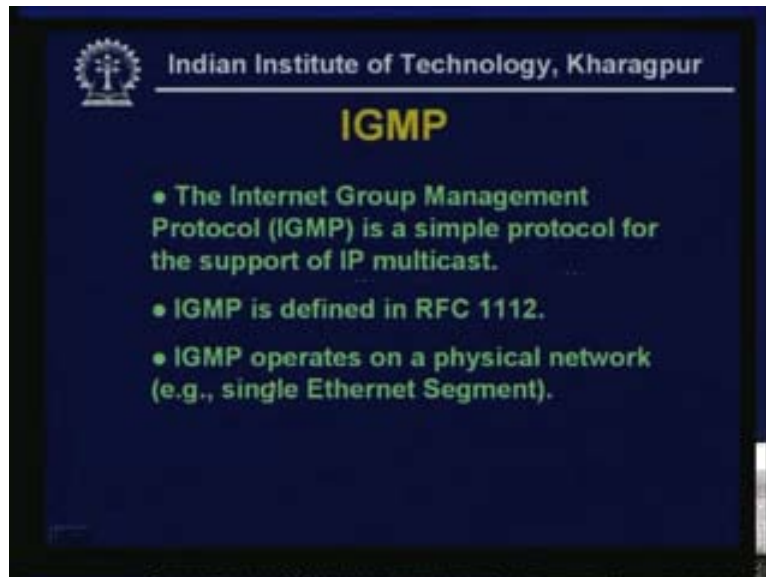
- Unfortunately not all Ethernet cards can filter multicast addresses in hardware. So, if it cannot be done in hardware then filtering is to be done in software by the device driver. So, you accept the packet and then do the filtering if it is multicast and if you are a member of the group and then accept it.

(Refer Slide Time: 14:19 – 15:49)



This is how the mapping is done. Suppose in this 1110, the first 4 bits and suppose this is the class D address and we are looking at the first byte of that address and the first four bits 1110 identifies that this is a class D address. Then this bit is actually ignored and then we have a 23 bit address. This 23 bit address comes straight to the Ethernet address. So these 7 bits, these 8 bits and these 8 bits are matched straight to the last 3 bytes of the Ethernet address. For the first three bytes of the Ethernet address we have a one here showing that this is multicast. Actually the Ethernet address with 01, 00, 5e in the first 3 bytes are reserved for IP multicast. So 01, 00 and this is 101 is 5e and 1110 is e. So, this is 01, 00, 5e and this is first 3 bytes, this is reserved for multicast and this part comes straight away.

(Refer Slide Time: 15:49 – 16:12)



- Now let us move on to IGMP which is the Internet Group Management Protocol. This is a very simple protocol for the support of IP multicast.
- IGMP is defined in RFC 1112.
- IGMP operates on a physical network that is the single Ethernet segment.

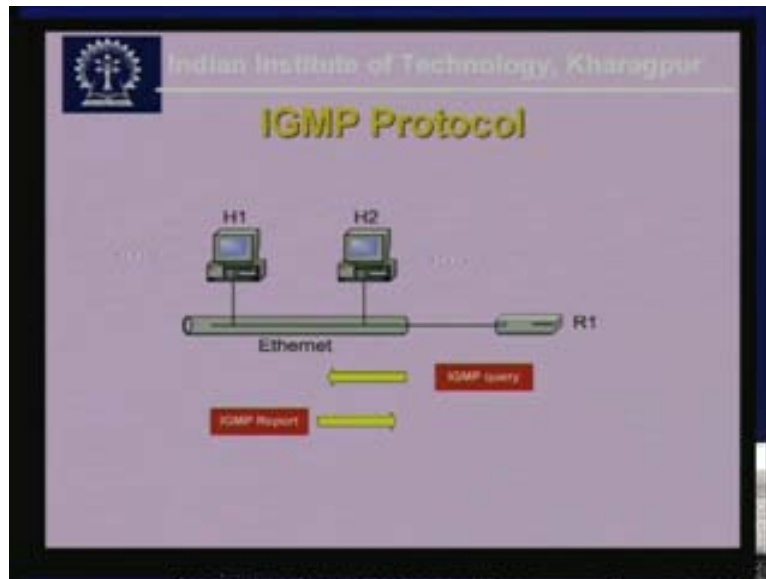
(Refer Slide Time: 16:12 – 17:08)



If you remember, in the previous diagram we saw that one particular router is connected to one Ethernet segment. So IGMP is between this router and the host which are there. So IGMP is used by multicast router to keep track of the membership. Now, who all amongst these members, who has ceased to be a member, who is the new person who

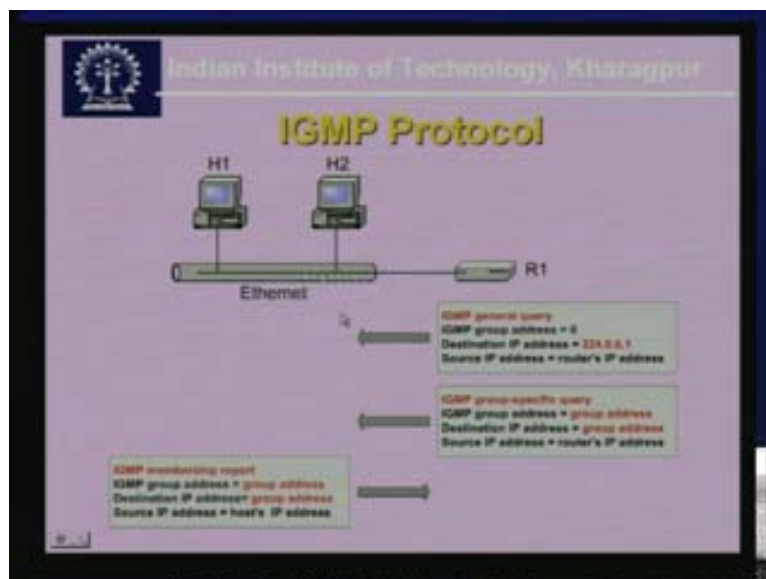
wants to join as a member, so this has to be kept track by the local multicasting router and that is what IGMP supports. So, it supports joining a multicast group, query membership and send membership reports. So the multicasting router will send queries from time to time and the host will respond or not respond depending on whether or not they are members of the group.

(Refer Slide Time: 17:08 – 17:27)



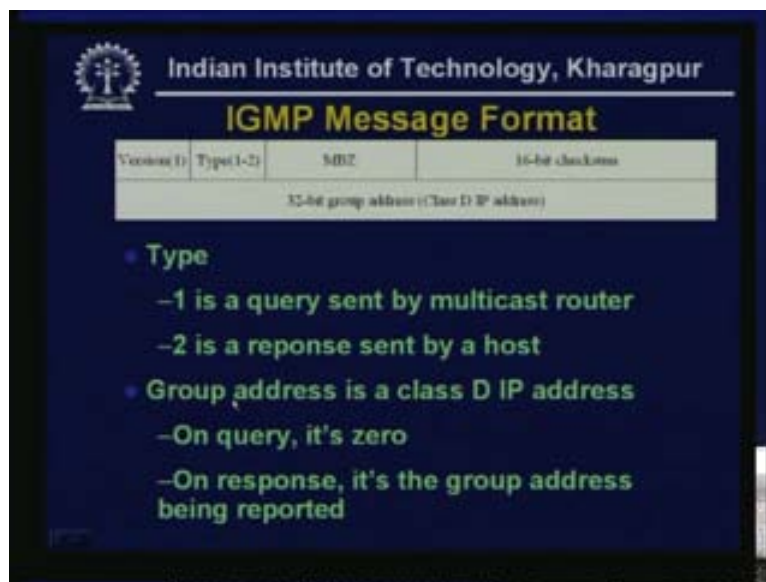
So, we have this multicasting router over here and one single Ethernet segment and number of machines connected there. So IGMP query comes from this multicasting router and IGMP report goes to the router from the host.

(Refer Slide Time: 17:27 - 18:30)



There may be an IGMP general query that IGMP group address is set to be equal to 0. It means that this query is for all the hosts, for all the groups and destination IP address is broadcast in this subnet. You remember that 224.0.0.1 is broadcast in this subnet and source IP address is the routers IP address. There may also be groups specific query in which case the IGMP group address is the group address, destination IP address is again the group address because now I want to give this query only to the members of one particular group and source address is the routers IP address. And this individual host sends the reports so it is the IGMP membership report. Therefore IGMP group address is the group address, destination IP address is also the group address and source IP address is equal to host's IP address.

(Refer Slide Time: 18:30 - 19:02)



In the IGMP message format there is a version and type. Type may be 1 or 2, version is usually 1 and then a 16-bit checksum and 32-bit group address. Type: 1 for the query sent by multicast router and 2 is a response sent by a host. Group address is a class D IP address. On query it is 0 and on response it is the group address being reported.

(Refer Slide Time: 19:02 - 20:27)



- A host sends an IGMP report when it joins a multicast group. (Note: Multiple processes on a host can join. A report is sent only for the first process). This means that when a host wants to join one particular multicast group then it sends an IGMP report to the router that it wants to join.
- On the other side when a particular host wants to leave a group, it does not want this multicast traffic any longer so when it wants to leave that group it does not do anything at all. Only thing is that when the next query comes for this particular group, for which it was a member then it will not respond. So this means that there is some kind of aging in the group membership list that the router would maintain. So, no report is sent when a process leaves a group.
- A multicast router regularly multicasts an IGMP query to all the hosts (group address is set to 0).
- A host responds to an IGMP query with an IGMP report. If somebody fails to respond then it is taken that he has left the group.

(Refer Slide Time: 20:27 - 20:51)



Indian Institute of Technology, Kharagpur

IGMP Host Reports

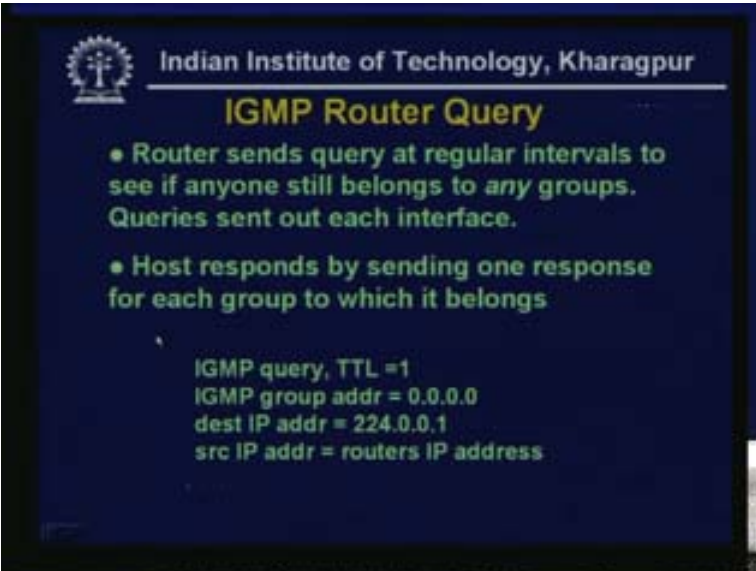
- Host sends a report when it joins a group
- Doesn't report when it leaves the group, but doesn't respond to next query

IGMP report, TTL = 1
IGMP group addr = group address
dest IP addr = group address
src IP addr = hosts IP address

What does the IGMP host reports look like?

- Host sends a report when it joins a group.
 - It does not report when it leaves the group but does not respond to the next query.
- So this is the IGMP report, the time to leave is 1, the IGMP group address is group address, destination IP address is group address and source IP address is host IP address.

(Refer Slide Time: 20:51 – 21:17)



Indian Institute of Technology, Kharagpur

IGMP Router Query

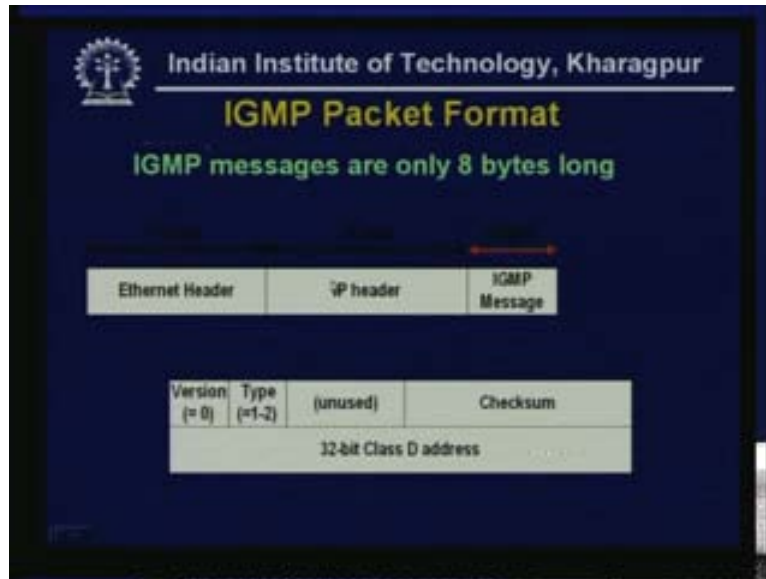
- Router sends query at regular intervals to see if anyone still belongs to any groups. Queries sent out each interface.
- Host responds by sending one response for each group to which it belongs

IGMP query, TTL = 1
IGMP group addr = 0.0.0.0
dest IP addr = 224.0.0.1
src IP addr = routers IP address

For general query, group address is 0, destination IP address is naturally broadcast and source is the routers IP address.

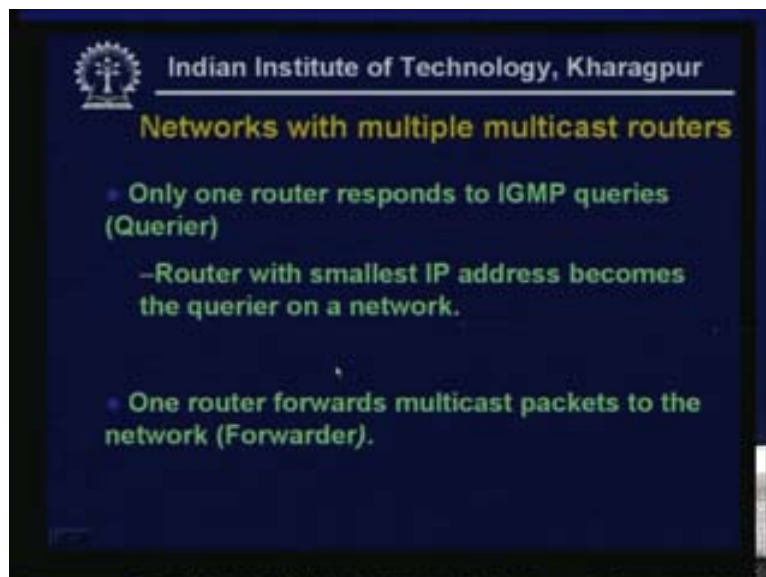
- So routers send query at regular intervals to see if anyone still belongs to any group. Queries sent out each interface.
- Host responds by sending one response for each group to which it belongs.

(Refer Slide Time: 21:17 - 21:36)



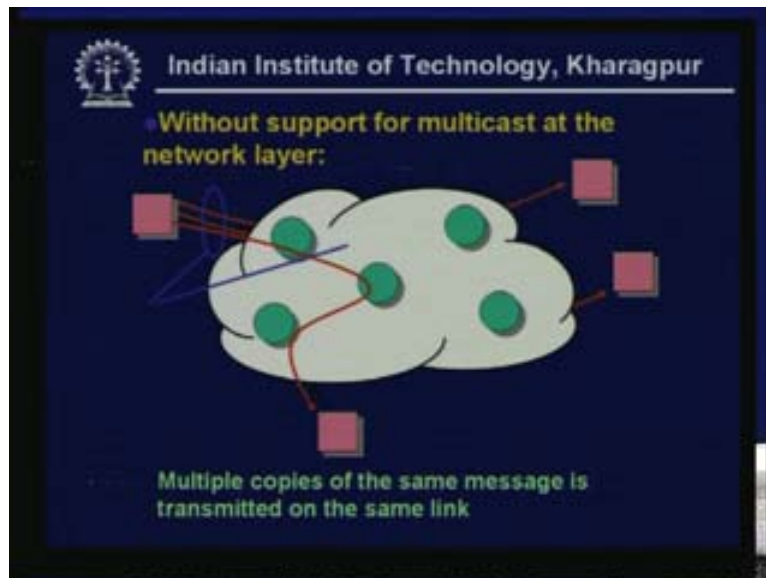
IGMP messages are only 8 bytes long. We have Ethernet header, IP header and the IGMP message which is version, type and some part is unused and the checksum and a 32-bit class D address.

(Refer Slide Time: 21:36 – 22:04)



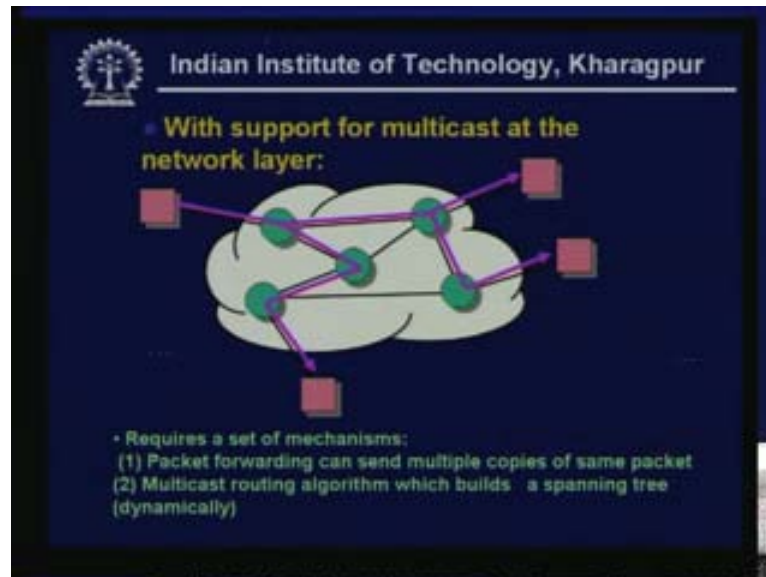
Suppose you have a network with multiple multicast routers. That means the same network but it has got multiple multicast routers. Only one router responds to IGMP queries so this is the Querier. So the router with the smallest IP address becomes the Querier on a network. One router forwards multicast packets to the network, so it is the forwarder. If a network happens to be so constituted that there are two routers connected to it and both of them support multicasting in that case, only one router will actually do the querying so out of these two routers whichever has the smaller IP address will be the one which does the querying. Now we come to the topic of Multicast Routing. So, what is special in Multicast Routing?

(Refer Slide Time: 22:38 – 22:52)



Let us see this diagram. Suppose there is no support for multicast at the network layer which is the case in many practical situations, even then you could sort of simulate multicasting by doing repeated unicast. So your original source has the list of all the members meaning all their IP addresses so it sends the message to all of them one by one, one by one, one after the other. So this is just a successive unicast done. Therefore this is as if a multicast. Obviously you are more packets are packed into hops if you take some measure like that and of course you are doing much more work than what is strictly necessary but this is all you can do. This has an advantage that the source can closely control that who could be a member of the group and who would not be a member of the group. Therefore you can impose some kind of access control by having an access list.

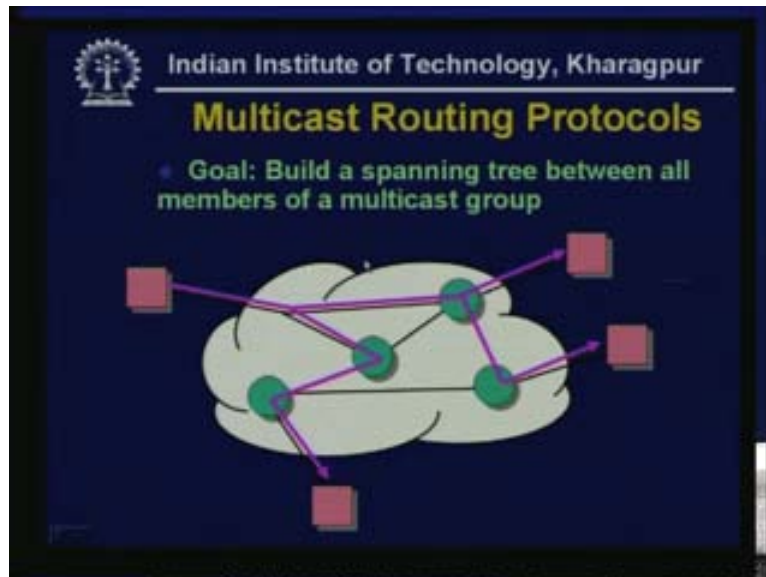
(Refer Slide Time: 24:05 – 26:37)



Now, if there is support for multicasting then what would happen is that, let us say there is one packet being sent to all three members of the group and say this is the source therefore the source will send only one packet to the next router. This router is going to duplicate the packet as to one on this link and the other on this link. This packet is ultimately destined for this host whereas this packet again gets multiplied and now this packet goes to this host and this packet goes to this host. So, the number of packets traveling down is minimized a lot, of course the final number of packets is the number of users but if you just consider how much each packet travels, that means if you take the number of packets into the hop count kind of a weighted measure then that could be much lower overhead in some sense for packets that are traveling. So it is much lower overhead on the links but may be more overhead on the routers.

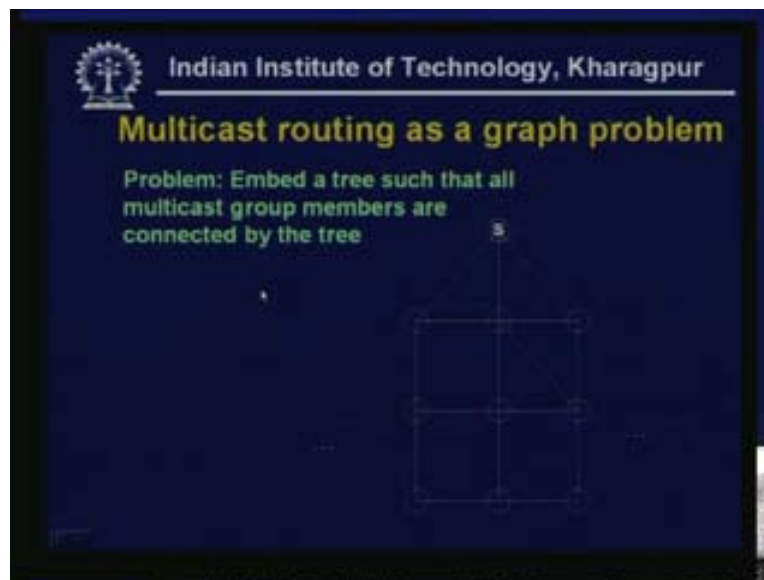
Now, if you have to have this multicasting capability for the routers this specifically requires two things. One is, packet forwarding that can send multiple copies of the same packet. For example, consider this router, this router is receiving only one packet but it has in its list that there are two sort of users for which the packet is supposed to go through this router. So it has to duplicate the packet one for this link and other for this link. So it forwards multiple copies of the packet. This capability has to be there in the router. Secondly, multicast routing algorithm builds a spanning tree dynamically. But how you found this tree? This looks somewhat similar to forming a routing tree for unicast cases but there are some differences. This tree has to be built up dynamically and in a distributed fashion by the routers. For that they have to run IP multicasting protocol between themselves. That is what we mean when we say routers are supporting multicasting.

(Refer Slide Time: 26:37 - 26:52)



Goal: The main goal of multicast routing protocol is to build a spanning tree between all members of a multicast group. So these are the members of the multicast group and we have to somehow get this tree.

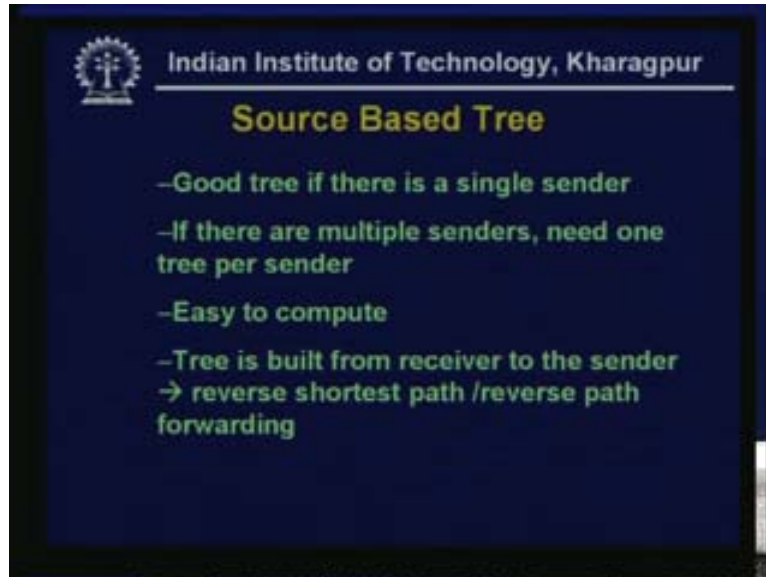
(Refer Slide Time: 26:52 - 27:57)



This can be looked upon as a graph theoretical problem. In whatever graph you have you have to embed the tree such that all multicast group members are connected by the tree. Suppose these are the three members of the multicast group seen in the previous graph and you want to form a tree like this then the only solution is to have a shortest path tree or source-based tree. That is, build a tree that minimizes the path cost from the source to

each receiver. So this is the so called source-based tree and you can form this. Hence this is one kind of a solution.

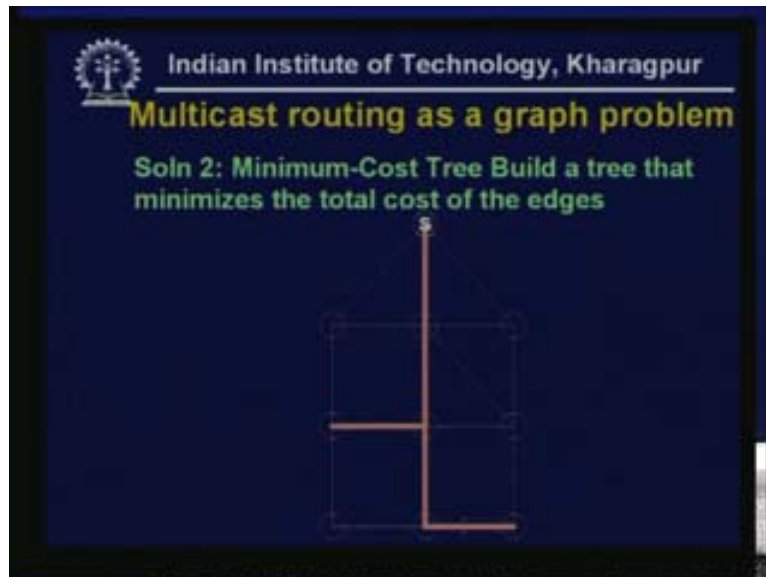
(Refer Slide Time: 27:57 – 30:24)



This is called a Source-Based Tree.

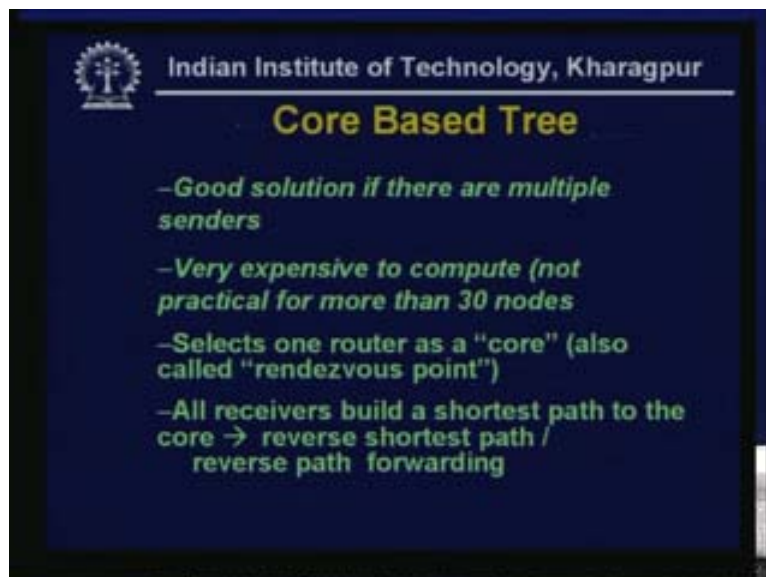
- This is a good tree if there is single sender. So sometimes multicast group is such that there is a single sender. Take the previous example we were talking about, a central news service or some kind of financial advisory service has some members and these are the members of this multicast group and there are some stock codes. So this particular group may be interested in the quotation of a particular group of stocks and for this particular group of stocks this company collects all the information, the stock value, etc in a regular fashion and keeps on pushing it to the members of this group. Now, this is multicasting where there is a single sender. And in such cases making a Source-Based Tree makes quite lot of sense. But of course, if there are multiple senders you need one tree per sender. Now that becomes really difficult where it becomes more democratic where all the group members are interacting and any of them can send messages to any member in the group. Therefore you have to have a tree for each sender. Having a single sender is easy to compute. For this multicasting router we will always assume that whatever unicast routing is happening through OSP etc is always present here but this multicast is sitting as an additional service by the router which essentially means that the unicast routing table is available for building up your Source-Based Tree. So in such a case this is easy to compute. The tree is built from receiver to the sender. This is called reverse shortest path or Reverse Path Forwarding (RPF).

(Refer Slide Time: 30:24 – 31:20)



A second solution to the same problem is that, if you remember the other graph, this graph looks different because this is the graph where it minimizes the total cost of the edges. If you do not know who your sender is going to be, that means if any member of the group can be a sender then it makes sense to make the tree in such a manner, suppose, if you assume that all of them send packets frequently then in that case having the tree with the minimum total cost of edges would be the optimum solution. So this is the second kind of solution.

(Refer Slide Time: 31:20 – 32:18)

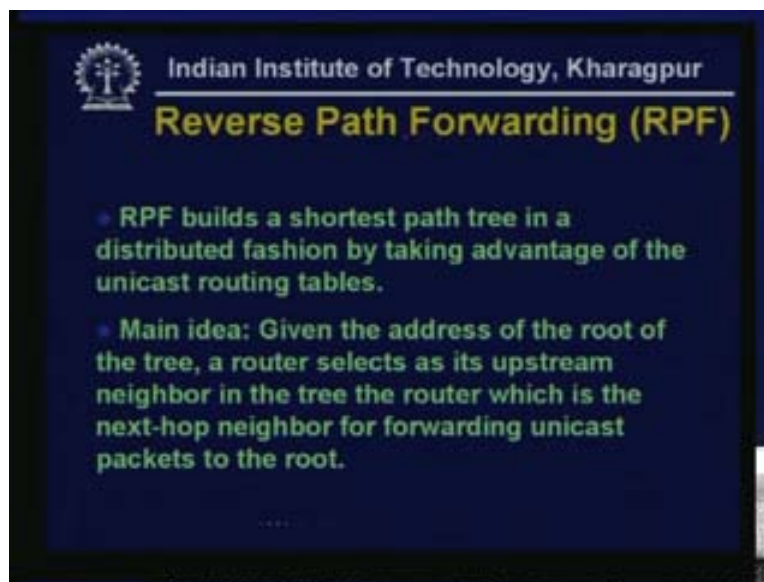


This is very difficult to compute, this is called the Core-Based Tree.

- This is a good solution if there are multiple senders. Instead of keeping one Source-Based Tree for each potential source we keep one Core-Based Tree.
- Very expensive to compute, not practical for more than 30 nodes for a very good solution.
- Selects one router as core (also called “rendezvous point”).
- All receivers build a shortest path to the core using the reverse shortest path or reverse path forwarding.

But who would be the core of the rendezvous point depends on how good your core based tree is thereby depending on how you choose the core. If you have chosen the core towards the center of the potential graph then that is good.

(Refer Slide Time: 32:19-34:26)



Let us see the details of Reverse Path Forwarding (RPF). This is the way to build the tree.

- RPF builds a shortest path tree in a distributed fashion by taking advantage of unicast routing tables.
- Main idea: Given the address of the root of the tree, you know the source. This tree is being formed from the sources. Each of the destinations, that means each of these potential recipients are trying to reach to the source and for that they use the unicast routing table which is already there in the router. So given the address of the root of the tree, a router selects its upstream neighbor in the tree, the router which is the next-hop neighbor for forwarding unicast packets to the root. So, what you do is, for each of the potential recipient you are trying to minimize the path cost from this recipient to the one single source. Right now for the Source-Based Tree you have one single source. Whatever you do for unicasting, while sending a message from this node to that node is what you have to follow. What the routers have to do is that, on the way suppose two different potential routes from two different recipients go through the same router then from this point onwards it is expected that this router to the final destination is actually

the source of multicast communication and there is only one path and the tree would be automatically formed. This is the basic idea of Reverse Path Forwarding.

(Refer Slide Time: 34:27-34:48)

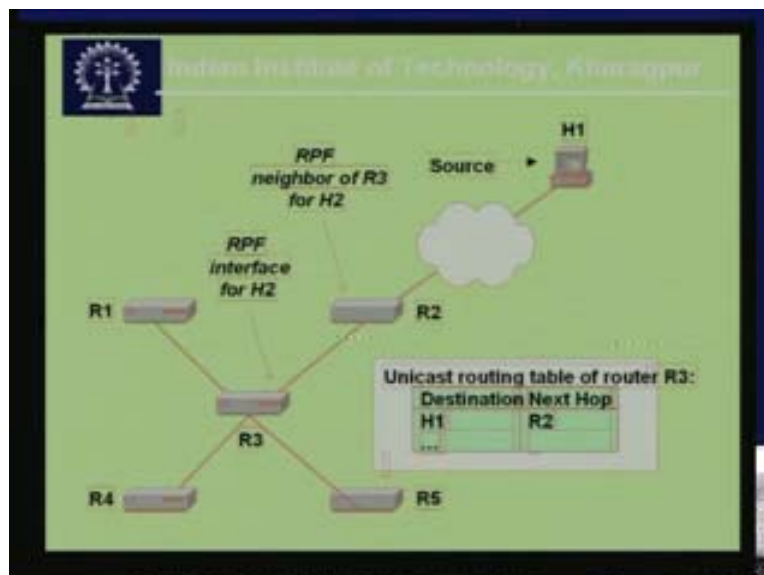
Indian Institute of Technology, Kharagpur

- How can this be used to build a tree?
- RPF Forwarding: Forward a packet only if it is received from an RPF neighbor

2. Set up multicast routing table in accordance from receiver to sender along the reverse shortest path tree

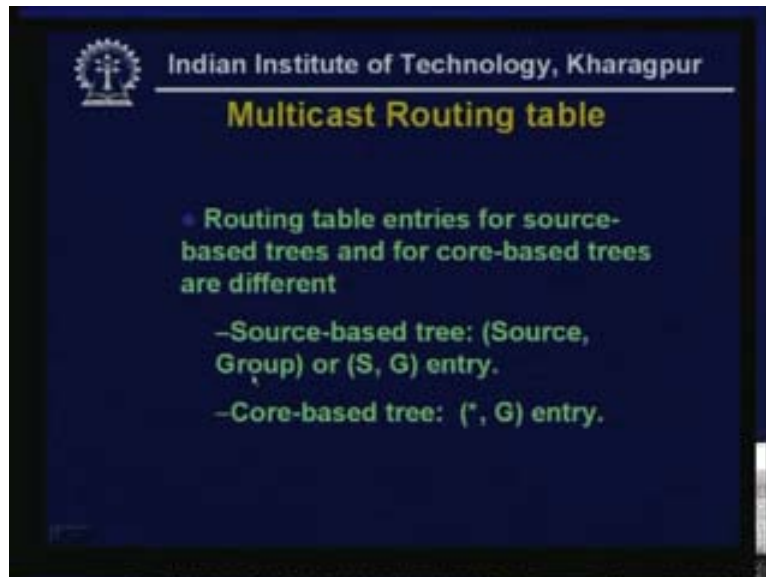
- How can this be used to build a tree?
- RPF Forwarding: Forward a packet only if it is received from an RPF neighbor.
- Set up multicast routing table in accordance from receiver to sender along the reverse shortest path tree.

(Refer Slide Time: 34:49-35:51)



This is an example. Suppose H1 is the source and RPF neighbor of R3, this is R3 and this is R1, R4 and R5. From these when they try to reach H1 they go from R3 to R2 to some path to H1. So R2 is the RPF neighbor of R3. The destination is H1 and the next hop is R2. This is the unicast routing table. So R3 knows that R2 is the RPF neighbor of itself.

(Refer Slide Time: 35:52 - 36:09)



- Routing table entries for Source-Based Trees and for Core-Based Trees are different.
- Source-Based Tree: For Source-Based Tree it is (Source, Group) or (S, G) entry.
- Core-Based Tree: Naturally anybody can be communicating. So it is (star, G) entry.

(Refer Slide Time: 36:10 - 36:49)

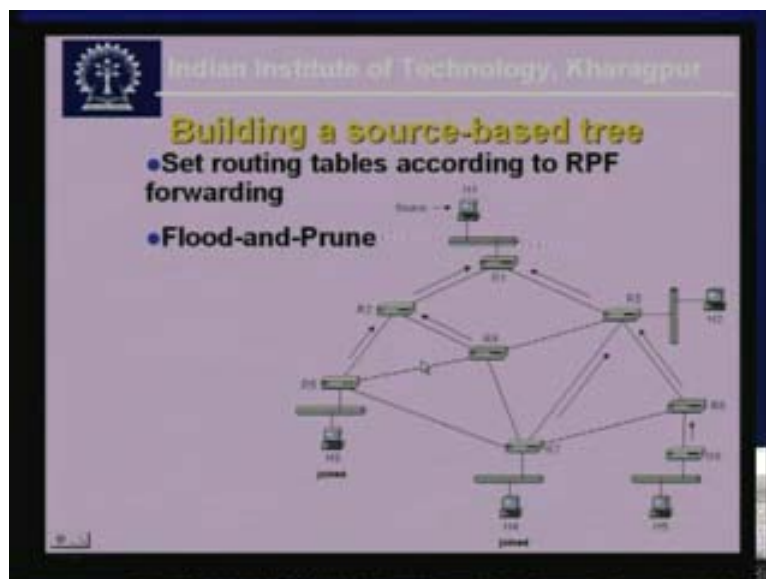


Indian Institute of Technology, Kharagpur

Source IP address	Multicast group	Incoming interface (RPF interface)	Outgoing interface list
S1,	G1	I1	I2, I3
*	G2	I2	I1, I3

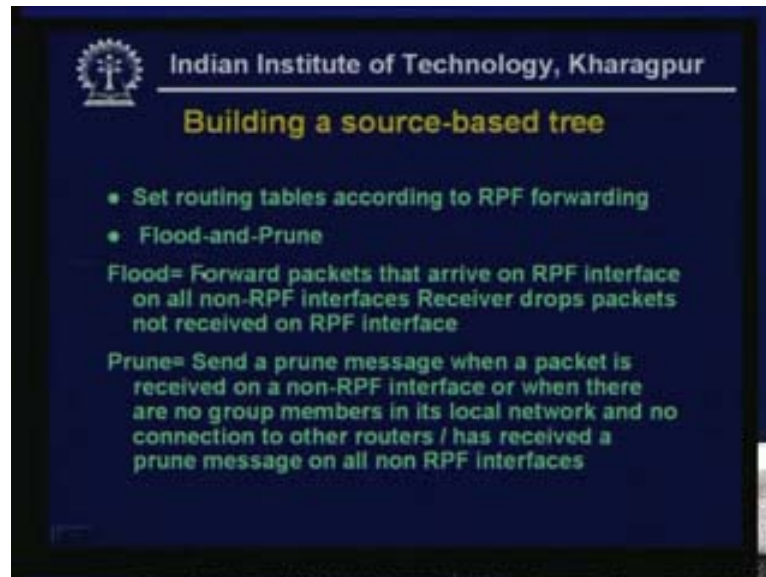
The Source IP address, Multicast group, Incoming interface (RPF interface) and Outgoing interface are the L2, L3 etc, this is a list. And finally when a packet arrives the router has to forward one copy of the packet along each of these outgoing links which eventually reach some members of this particular multicast group.

(Refer Slide Time: 36:50 - 37:08)



For building a Source-Based Tree in a network like this set routing tables according to RPF forwarding and then use Flood-and-Prune.

(Refer Slide Time: 37:09 - 39:43)



- Set routing tables according to RPF as we have already discussed.
- Flood-and-Prune.

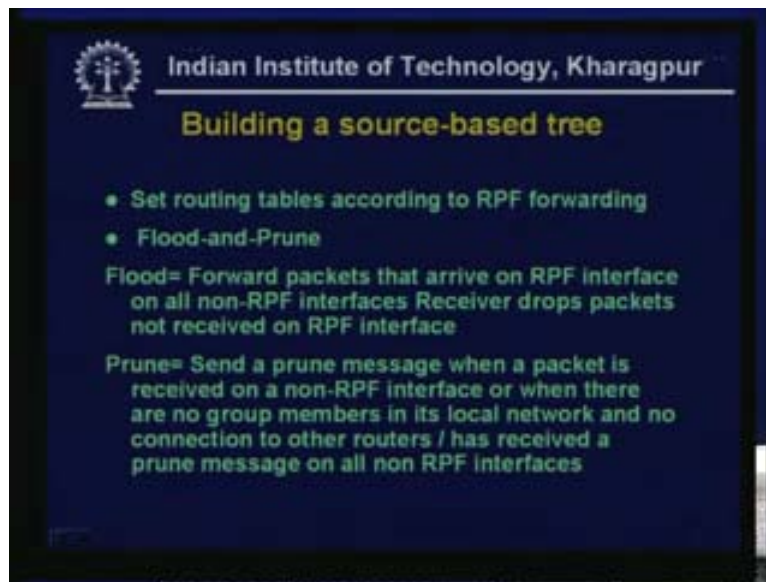
What is flood? Forward packets that arrive on RPF interface on all non-RPF interfaces. Receiver drops packets not received on RPF interfaces. These routers require the capability of forwarding multiple copies of the same packet. So, if a packet has come from its RPF neighbor, (RPF neighbor is with respect to a particular group) bearing this address means that it is actually coming from the source. Now it has to be forwarded to each of the outgoing interfaces. Of course it is a non-RPF. This means, when I say RPF interface it means that the RPF neighbor is coming from the source side to all others which lead to different members of this Multicast group.

What happens if you happened to get a packet from a link for this particular group who is not your RPF member? First of all, how did it happen? You must remember that we are doing this in a distributed and dynamic system so things can come up and go down. So that way a packet can come in. But obviously so far as this particular router is concerned if a packet comes from non-RPF link for this group then this is not coming from the source so that packet is dropped. And naturally it also does pruning. Pruning is sending a prune message when a packet is received on a non RPF interface. This is one case when you prune. Or when there are no group members in its local network and no connection to other routers.

Suppose, it so happens that this particular router, you remember that this router is also connected to its local network and with the host in the local network it is running IGMP always finding out who are the members of group etc. It could happen that this local member has retired. It no longer wants to remain in the group that means it is no longer sending your IGMP reports. So it has nobody to send it to nor is it connected to neither any router nor a part of a link from a distant source to a distant destination, nor a transit link like that. So it is not connected in that case also. Now as the local contributor

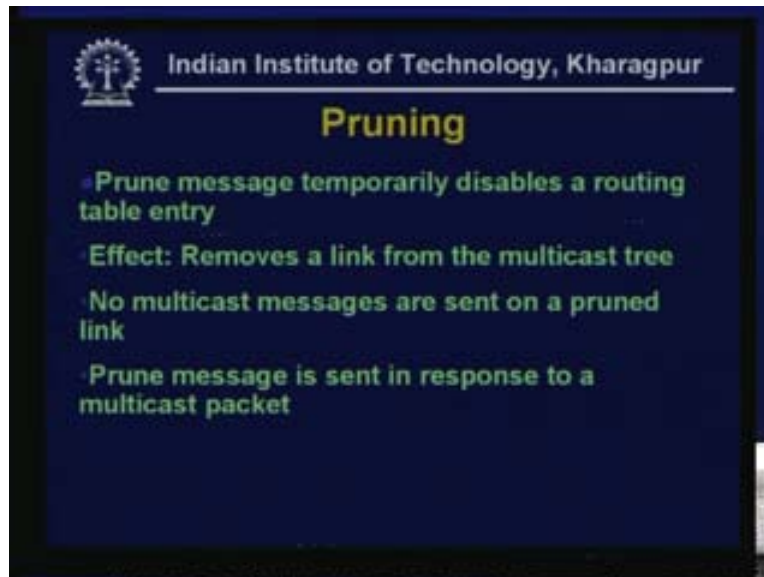
member of the prune has retired then this of course may not be known to others. So it may still get a packet but then what it will do is that, it will send a prune message stating not to send anymore packets to it any longer. So it will send the prune message along the route because the neighboring router has sent in a packet and it has nobody to distribute it to nor is it a transit router. So, naturally it drops this packet because it has no use for this packet. And along this link whoever has sent this packet to it the local member sends a prune message. It means do not send the local member any further packets because it has nothing to do with this group anymore.

(Refer Slide Time: 41:23 - 42:24)



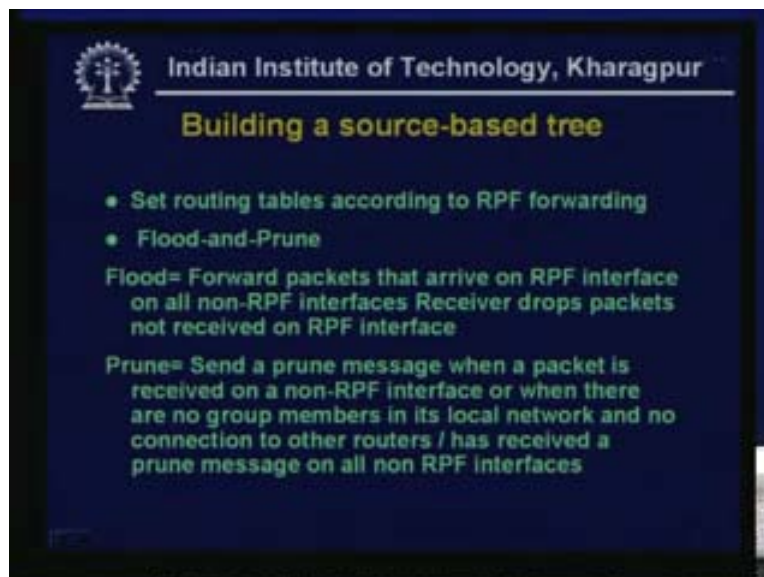
So that is one case, or, has received a prune message on all non RPF interfaces. That means, it was a member earlier with all the non RPF interfaces and just like the group member may have retired similarly this may also have been a transit router on a link from some distant source to distant destination this may be an intermediate router on the way. But then it has got a prune message on all its non RPF interfaces. That means it was a member of a transit link earlier but now it is no longer a member. So once again whoever had sent it a packet, it will send back a prune message to that destination that prunes this link as well. So this is no longer interested.

(Refer Slide Time: 42:25 - 42:51)



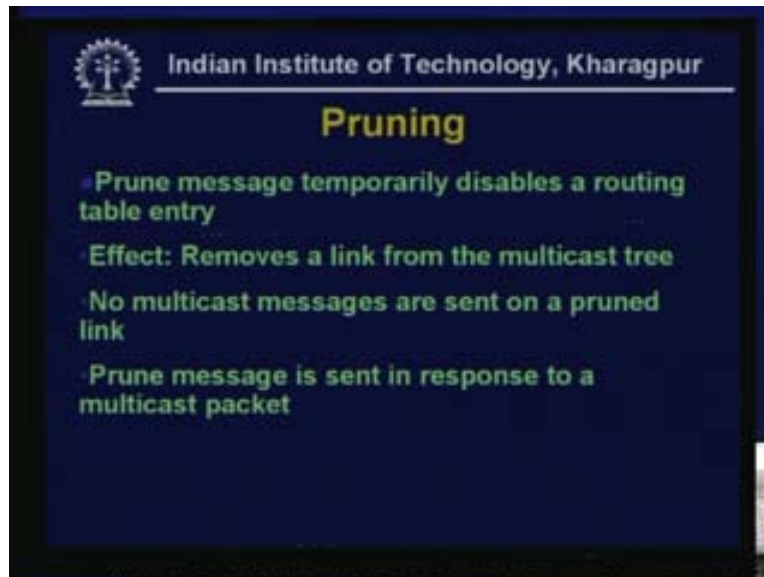
- Prune message temporarily disables a routing table entry.
- Effect: Removes a link from the multicast tree.
- No multicast messages are sent on a pruned link.
- Prune messages is sent in response to a multicast packet, which has come and which satisfies any of these conditions.

(Refer Slide Time: 42:52 - 43:07)



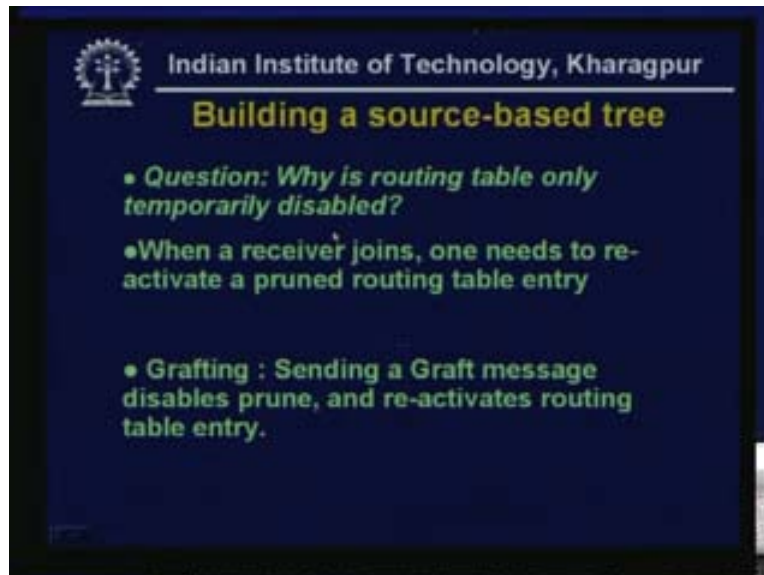
Once again that it has received on the non-RPF interface or when there are no group members in its local network and no connection to other routers or it has received a prune message on all non RPF interfaces. So in such cases the prune message is sent.

(Refer Slide Time: 43:08-43:19)



The prune message has the effect of temporarily disabling a routing table entry. The question is, why temporary?

(Refer Slide Time: 43:20 - 44:16)

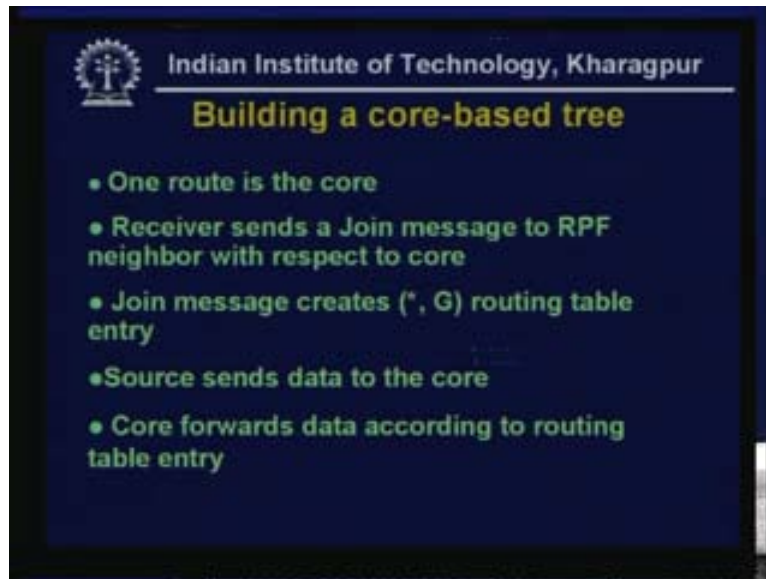


- Why the routing table is only temporarily disabled?
- What happens is that, you may have a receiver who may again like to join. So one needs to reactivate a pruned routing table entry in that case. So what happens is that, this group member may have gone away somewhere and now has come back and wants to be a member of the group once again. So, it gets the IGMP report saying that it is a member of this group. Now, it is aware of who knows the source, this multicasting router. So what

it will do is that it will try to reactivate this link and then the rest of it will work, so this is called Grafting.

- Sending a Graft message disables prune and reactivates the routing table entry. So this pruning and grafting are complimentary to each other. You prune to disable and you graft to enable again.

(Refer Slide Time: 44:17 - 45:50)

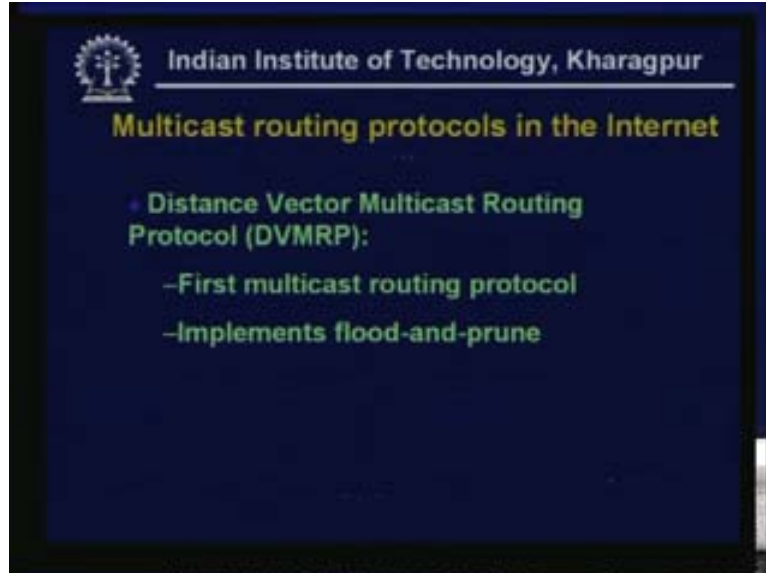


Next is the Core-Based Tree. This was a Source-Based Tree when you have one source and many receivers. Now you have many to many kind of situation. That was one to many communications, not one to all (not broadcast). But now we have many to many communications. That means there are many members of the group who might like to communicate with other members of that group. In this case we would like to have what is known as a Core-Based Tree.

- One router is the core.
- Receiver sends a join message to RPF neighbor with respect to core. Now every receiver actually wants to join to the core.
- Join messages creates a (star, G) routing table entry.
- Source sends data to the core.
- Core forwards data according to routing table entry.

Now, since there is no source or that anybody could be a source we put a star in place of s. For a particular router all the links get messages like this so a message may come in through any such link and it has to be forwarded to the other links.

(Refer Slide Time: 45:59 - 46:47)



We just mentioned about multicast routing protocols which is actually implemented in most of the routers and many of the level 3 switches. This is called DVMRP. So you find them actually but unfortunately I have seen it very rarely being used. But this is there in most of the routers of today as well as in many of the Level 3 switches DVMRP is there

- DVMRP is a Distance Vector Multicast Routing Protocol.
- This is the first multicasting routing protocol.
- It implements flood and prune.

Distance vector routing, if you remember, the distance vector routing uses the distributed Bellman Ford algorithm which is implemented by RIP. The centralized diesters algorithm, the link state algorithm is implemented in the routing protocol called OSPF.

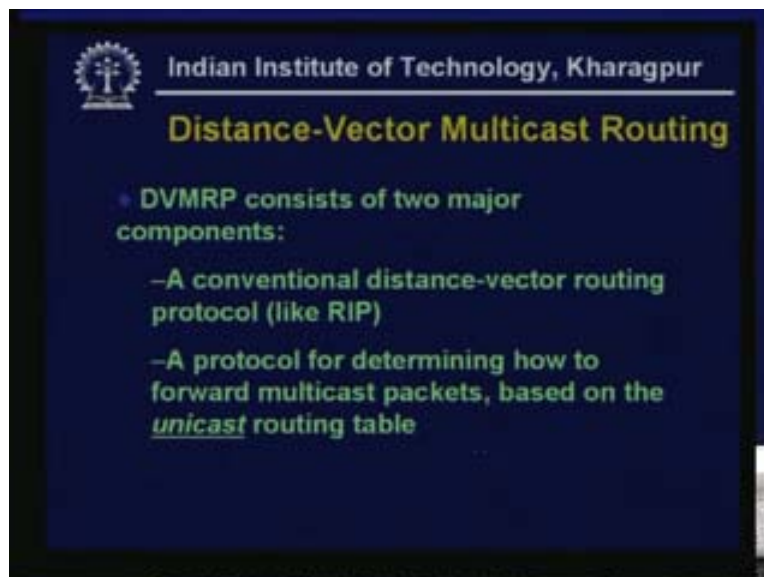
(Refer Slide Time: 46:48 - 47:58)



Open Shortest Path First: Recall our discussion about routing protocols and this OSPF is currently the most acceptable routing protocol. There is a multicast extension of OSPF which is known as MOSPF (Multicast Open Shortest Path First).

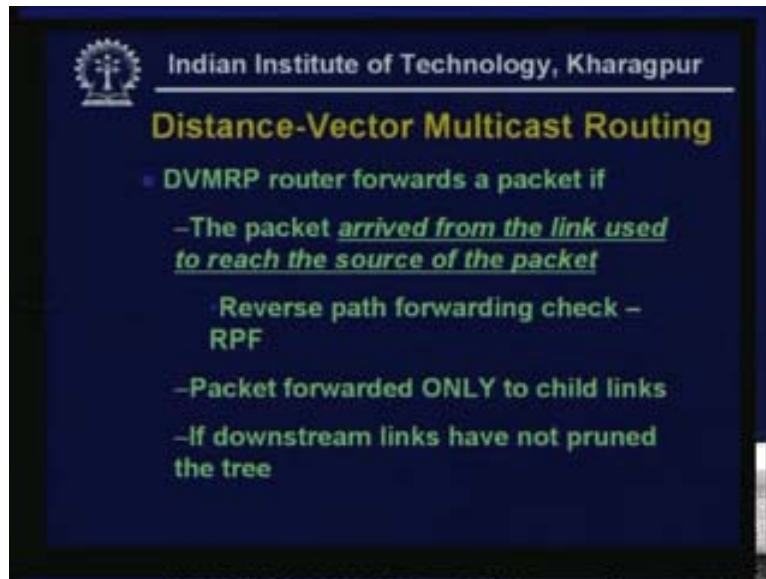
- Multicast extensions to OSPF: Each router calculates a shortest path tree based on link state database.
- It is not very widely used.
- PIM-SM builds Core-Based Trees but they are not widely used.

(Refer Slide Time: 47:59 - 48:18)



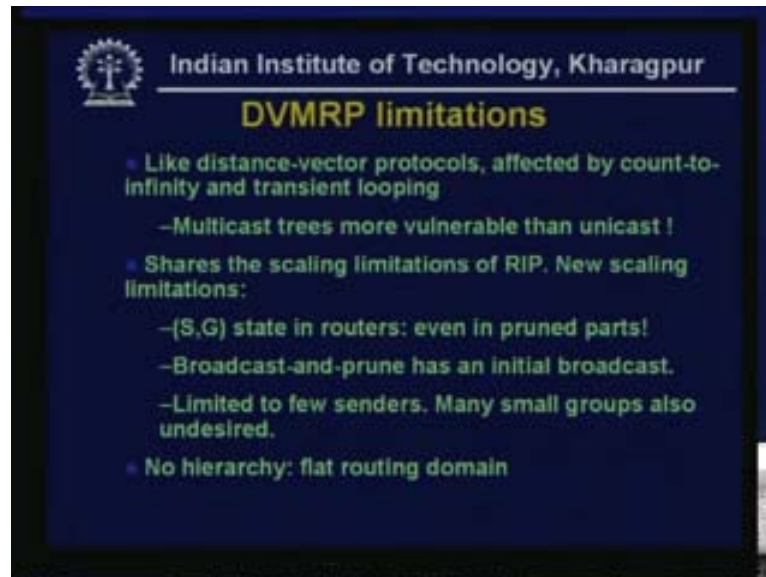
- Distance-Vector Multicasting Routing (DVMRP) consists of two major components:
 - A conventional distance-vector routing protocol (like RIP).
 - A protocol for determining how to forward multicast packets based on the unicast routing table.

(Refer Slide Time: 48:20 - 49:27)



- DVMRP (Distance-Vector Multicasting Routing) routers forward a packet if:
 - The packet arrived from the link used to reach the source packet. This is the reverse path forwarding. That means if from this router I want to reach the source then I have to go to that next hop and that is my RPF neighbor. So, if the packet arrives from this link from my RPF neighbor link, arrived from the link used to reach the source of the packet then this is the RPF chain.
 - Packet forwarded only to the child links not in the direction from which it came but other child links.
 - If provided the downstream links have not sent a prune message.

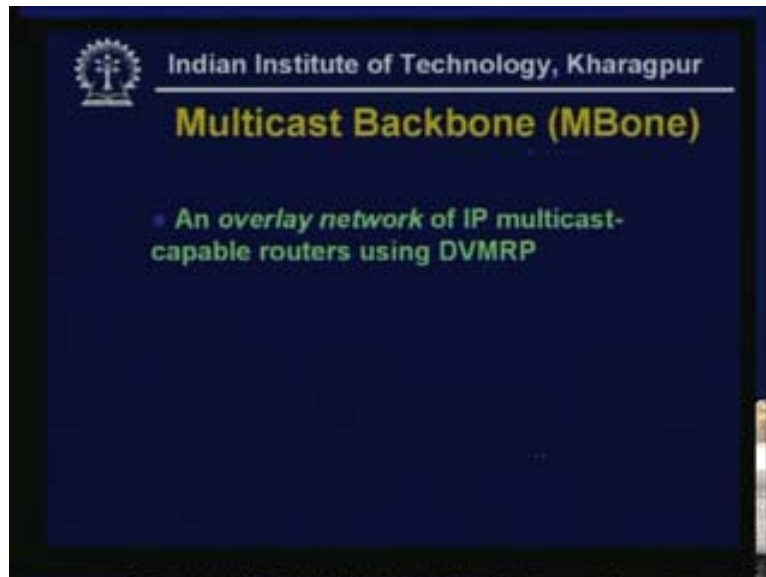
(Refer Slide Time: 49:28 - 52:45)



But DVMRP has limitations:

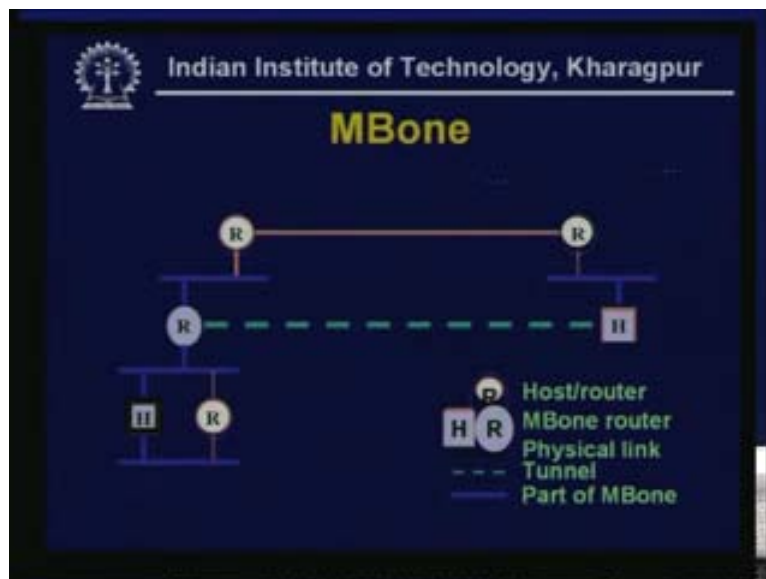
- Like distance vector protocols, affected by count-to-infinity and transient looping. In the count-to-infinity problem some link has failed but nobody could make out that the link has actually failed so it is going round and round known as the count-to-infinity problem where exactly the counting of potential distance to that link comes to infinity. Since we are using the same distance vector routing. Transient looping means sometimes a routing loop may form and the packet goes round and round.
- Multicast trees are more vulnerable than unicast for these problems.
- This shares the scaling limitations of RIP. And this scaling limitation essentially comes from what I have written in the last.
- No hierarchy: Flat routing domain. One of the advantages of OSPF over RIP was that in OSPF we break up the network into a hierarchy. There are these autonomous regions or autonomous domains and then further down it can be broken up so that the routing problem remains simpler and you can scale to bigger and bigger networks. Since DVMRP is based on RIP or essentially on the ideas of RIP it is again a problem in DVMRP also. Here you cannot scale and then you have further problem because of multicasting.
- You may have (S, G) state in routers: even in pruned parts.
- Broadcast-and-prune has an initial broadcast. When I say flood-and-prune, actually you are flooding the network so there is some kind of broadcast going on. If the network size is small, this broadcast may be acceptable but when the network grows bigger and bigger broadcast becomes unacceptable. So that is again another problem in scaling.
- This is limited to few senders. Many small groups also undesired. Since this essentially forms a Source-Based Tree you can have only a few of them, just a few senders. Many small groups are also undesired. If you have large number of groups, once again you have the same problem of maintaining so many trees and that also becomes a limitation for scaling.

(Refer Slide Time: 52:46 - 53:29)



Let us discuss about an effort to implement multicasting. As I told you, most of the routers are not configured to use the multicast in every manner but still some people want to use multicasting. So they built up this Multicast backbone (MBone) which is essentially an overlay network of IP multicast-capable routers using DVMRP. So it uses DVMRP and it is an overlay network of IP multicast-capable routers.

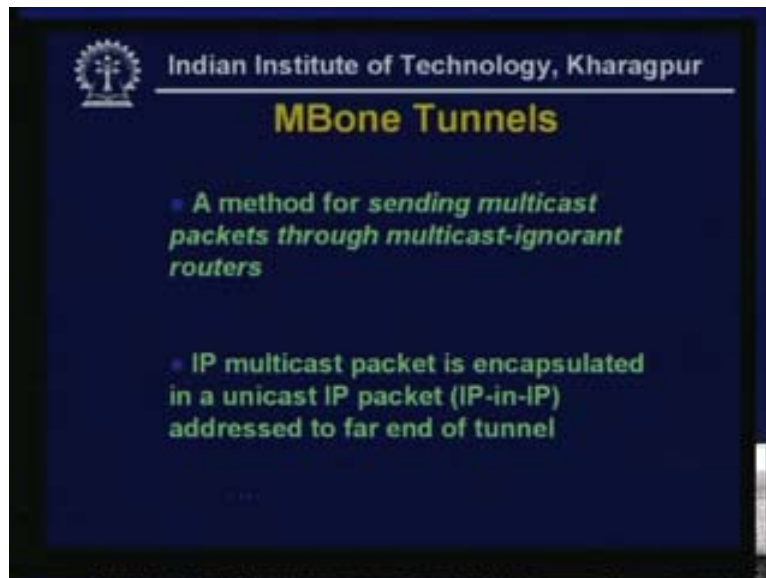
(Refer Slide Time: 53:30 – 55:05)



What does that mean? That means some of the routers in the network in some places are multicast-capable. And what happens is that they are going to support multicasting in its own locality. That means it will support multicasting amongst the network to which they

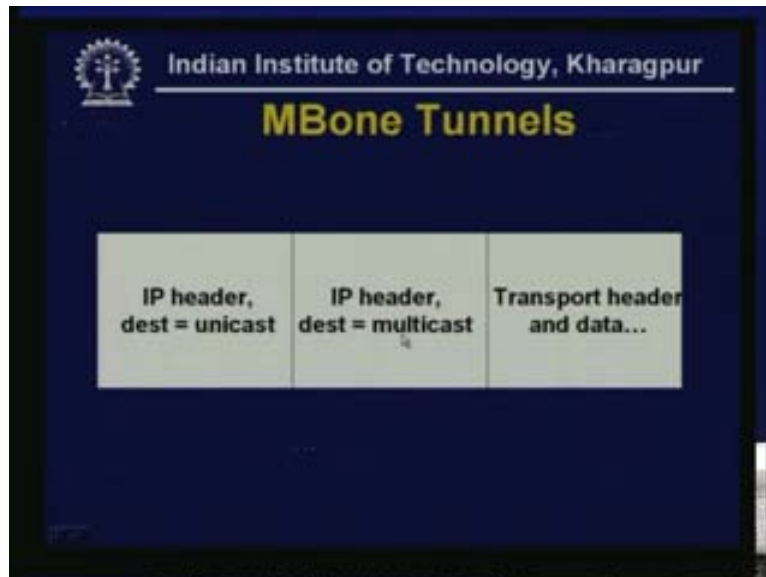
are directly connected. These routers are going to run a multicasting protocol between themselves. But then in between there are whole lot of other routers. In between there is a cloud of routers which are not supporting multicasting so what it will do is that it will tunnel through this cloud to the next multicast supporting router. So this is the picture of the MBone. You have R which is the host or the router and this R and this H are the MBone routers. They support and the part of the MBone is shown in light blue where the multicasting is directly supported whereas when they try to communicate to another multicast supporting node over a cloud which does not support multicasting they tunnel through it.

(Refer Slide Time: 55:08 - 55:18)



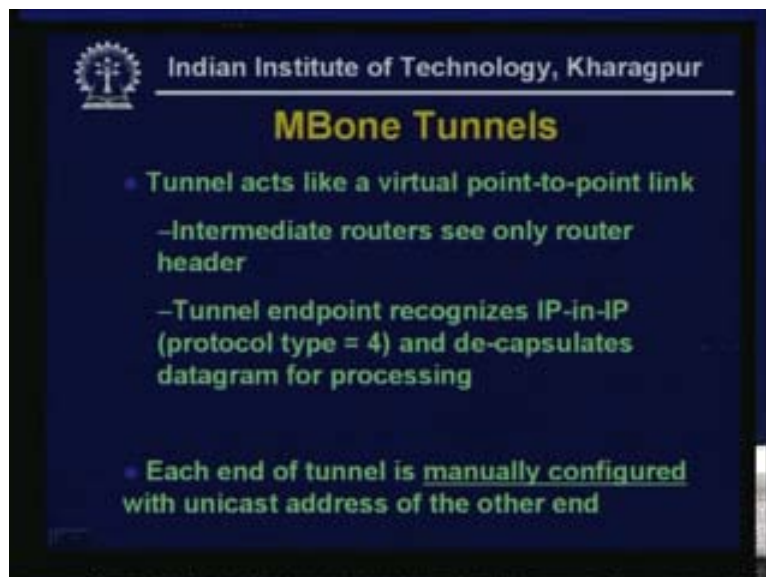
- MBone tunnel is a method for sending multicast packets through multicast-ignorant routers.
- IP multicast packet is encapsulated in a unicast IP packet (IP-in-IP) addressed to far end of the tunnel.

(Refer Slide Time: 55:21 - 56:07)



You have the IP header destination which is unicast and then you have another IP header destination that is multicast and then the transport header. What happens is that, the intervening routers which are not multicast-enabled are going to see this destination and this destination would then actually be the next multicast router. And here this part will be the payload so the network nodes would not look into this. When it reaches the next multicast supporting router it will get this and then discard this and then look at this multicasting header. So this is the IP-in-IP encapsulation and tunneling.

(Refer Slide Time: 56:07 - 57:23)



- Tunnels act like virtual point-to-point link.

- Intermediate routers see only router header. That means the unicast routing header.
- Tunnel endpoint recognizes IP-in-IP (protocol type equal to 4) and de-capsulate the datagram for processing.
- Each end of the tunnel is manually configured with unicast address of the other end.

This is what you have to do. This was done to implement multicasting in an environment and try it out. If there are problems about the one which is actually implemented in most of the routers namely DMRP that does not scale well and if there are many groups, in today's world when everybody in sort of networked and people have all their special interest etc it is quite considerable that the number of groups will explode if it could really do multicasting in a very easy fashion and that is very difficult for routers to handle. That is why most of them do not use it at the moment. But potentially this is a very useful kind of technology. Thank You.