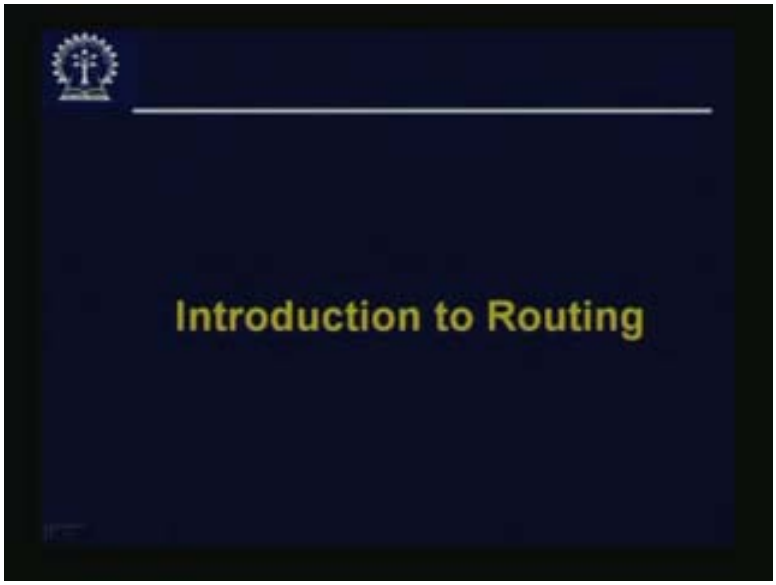
Computer Networks
Prof. Sujoy Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture - 26
Introduction to Routing

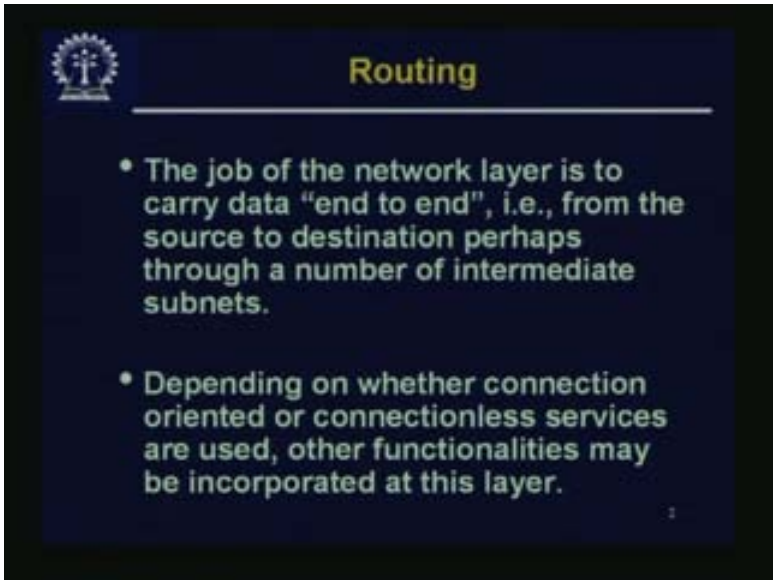
Today we will start our discussion on routing. We have already talked about routing a little bit in different context, specifically in the context of ATM of how the ATM virtual path etc are set up. Today we will start our discussion on the major area of routing and especially with reference to the TCP/IP stack. That is how packets are routed in an IP network.

(Refer Slide Time: 01:22 - 01:33 min)



Today we will start the introduction with routing and then we will take up the discussion about different routing protocols in the next set of lectures.

(Refer Slide Time: 01:34 - 03:46 min)

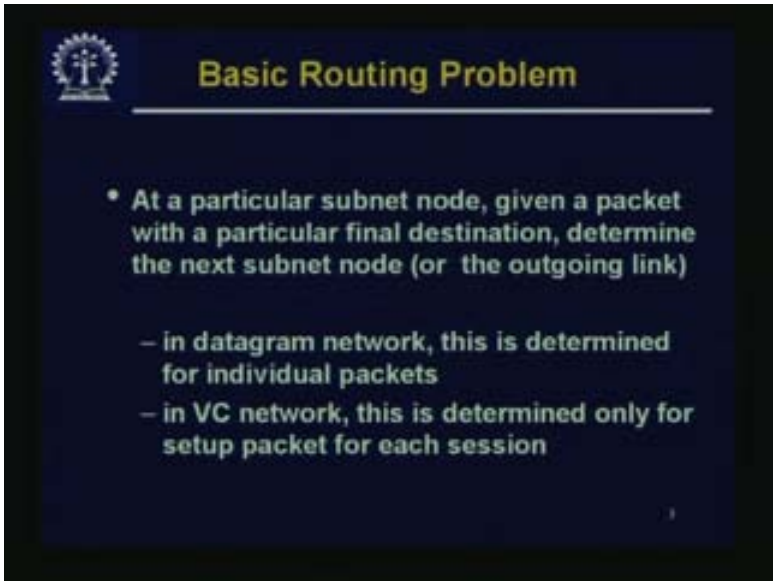


Let us just recollect, what is the job of the network layer or what is routing? The job of the network layer is to carry data from end-to-end. That is, from the source to destination perhaps through a number of intermediate subnets. Now depending on whether connection-oriented or connectionless services are used other functionalities may be incorporated at this layer.

We will talk about this later on. Right now we are talking about routing of IP packets and later on we will discuss on how you can have a virtually connection oriented system on that. Unlike data link layer, if you remember, is just the next hop, just the link which is immediately adjacent. So that has some advantages in the sense that whatever information you require about it are locally available.

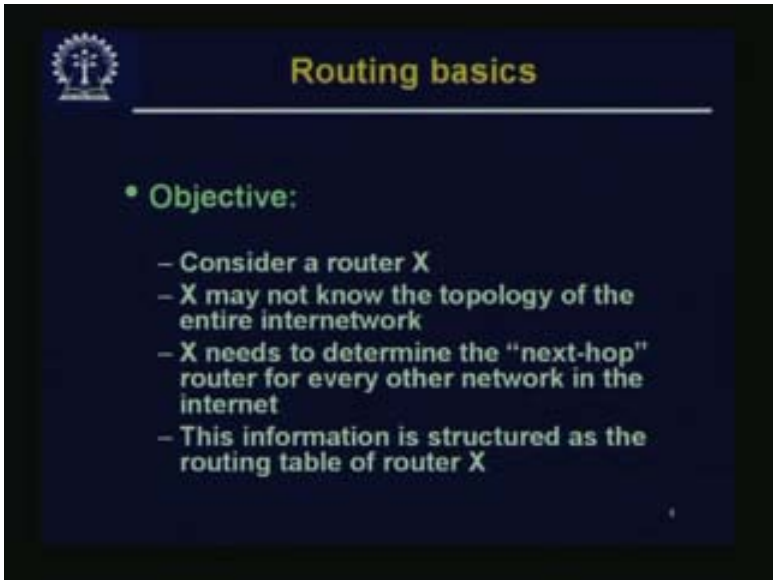
Unlike the data link layer, the major problem with routing is that it happens over multiple networks and towards a very remote system and the packet might have to take many hops, may be 10, 20 or even 30 hops to reach the end point. When you take 20 hops the area you are serving becomes so large with so many machines connected to it. And then how do you keep track and then switch so many machines with so many links? The problem is some of the links may go down, some of the machines may go down, some of the machines may come up and when I may refer it actually says PCs, servers, etc, they may also refer to network boxes like other routers. So the job of the router is to know which link it should take so that globally the packet will arrive nearer to its destination.

(Refer Slide Time: 03:47 - 04:12 min)



This is the basic routing problem. At a particular subnet node given a packet with a particular final destination determine the next subnet node or the outgoing link which is appropriate. In the datagram network this is determined for individual packets but in VC networks this is determined only for setup packet for each session. Now we will concentrate on the datagram network.

(Refer Slide Time: 04:13 - 08:20 min)



Consider a router X. X may not know the topology of the entire internetwork. These days everybody wants to be connected to the internet so we have a giant network of networks. So there is this big network of networks spanning the entire globe and then a particular network once again may be divided into so many sub networks.

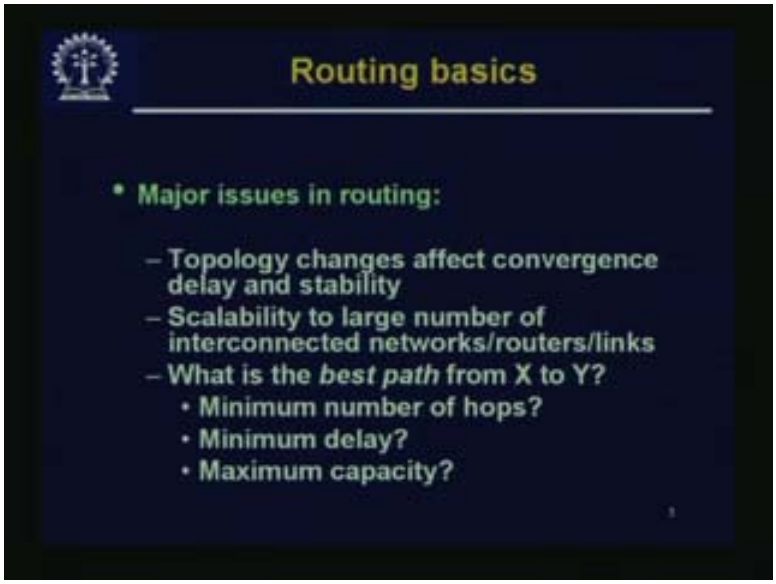
There are billions of machines connected to this network so some user somewhere wants to connect to another user on the other part of the globe. This is a huge problem that must be solved in a systematic manner. But this is the objective of routing or the network layer. So X needs to determine the next–hop router for every other network in the internet. We are trying to reach some particular machine, some particular server. If you want to keep track of all the machines in the world it becomes really impractical. We somewhat reduce the problem where all these different machines are grouped into different networks or even sub networks. They are grouped into different networks so that a remote router needs to keep track of only the remote network rather than a particular server in that network.

Of course, the idea is that, once you reach your destination network finding a particular server within that network will be very easy. Either through ARP or some such protocol you can reach the particular server once you have reached the correct destination network. The entire information that is required is structured as a routing table of router X to keep track of all the other networks.

What is a routing table? Given the address of a particular network in a remote location we should be able to find from the routing table that which local hop I must take next. Even that is not easy even if you reduce the scope of the problem from servers or PCs to networks because there are millions of networks in the world. So theoretically if you do it in a very naive fashion you have to keep millions of entries so that you can match and know that this is what the mistake is. Of course, even this is not possible because at the same time you want to go to the correct destination for this particular packet and at the same time you want to process the packets as fast as possible.

People want more and more speed so the network traffic and the number of packets are increasing day by day so you have to process the packets very fast. If you have a very large table then it demands time even just to look up to it and you require a lot of memory. Additionally it consumes lot of processing power which will thereby drive up the cost of the router. So, even keeping millions of entries for most routers this is not a feasible option therefore we have to do something about it.

(Refer Slide Time: 08:21 - 10:04 min)

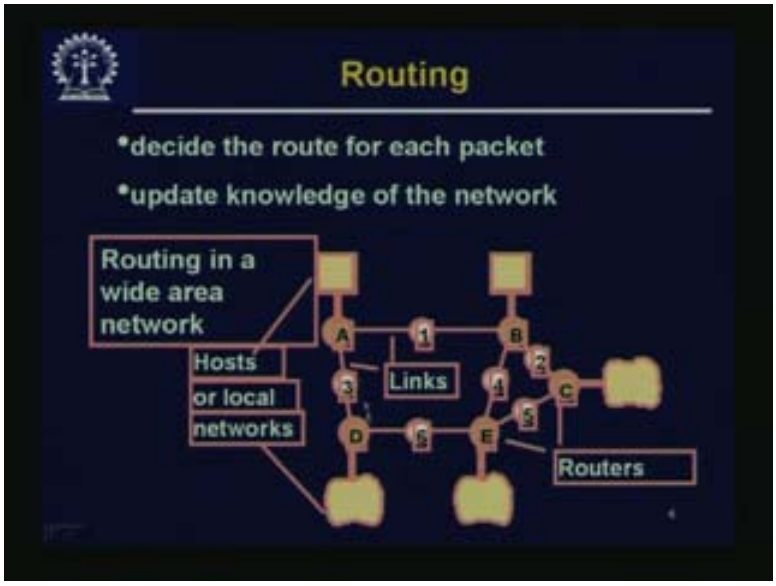


The other issues in routing are: One is, the topology changes affect convergence, delay and stability. Topology of the network changes all the time because the links may go down or come up, nodes may go down or come up so the topology is changing. Therefore this may the change the path that a particular packet takes and the path the next packet takes in the same stream. This may affect the delay and the stability.

The other problem is scalability to a large number of interconnected networks or routers or links. And even when you come down from nodes to networks this is still a very large problem. Then there are other issues like what is the best path from X to Y. It may be that five different routes are possible from X to Y.

Now all these five routes are not equal. First of all they may not be equal in the number of hops, they may not be equal in length, they may not be equal in cost, they may not be equal in the quality, some of the routes may be very unreliable that the packet has a larger probability of getting dropped and so on and so forth. So we would like to have the minimum number of hops or the minimum delay or the maximum capacity. Therefore if possible we would also like to incorporate the quality of the path when deciding on a route for a particular packet from X to Y.

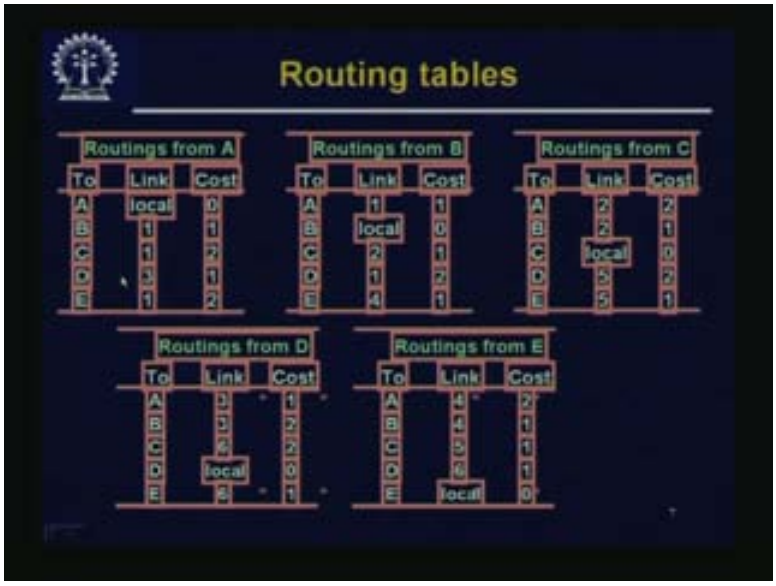
(Refer Slide Time: 10:05- 11:30 min)



So routing consists of deciding the route for each packet. And in order to do that the router has to have knowledge of the entire network and this knowledge has to be dynamic because the network topology keeps on changing so we have to update the knowledge of the network from time to time.

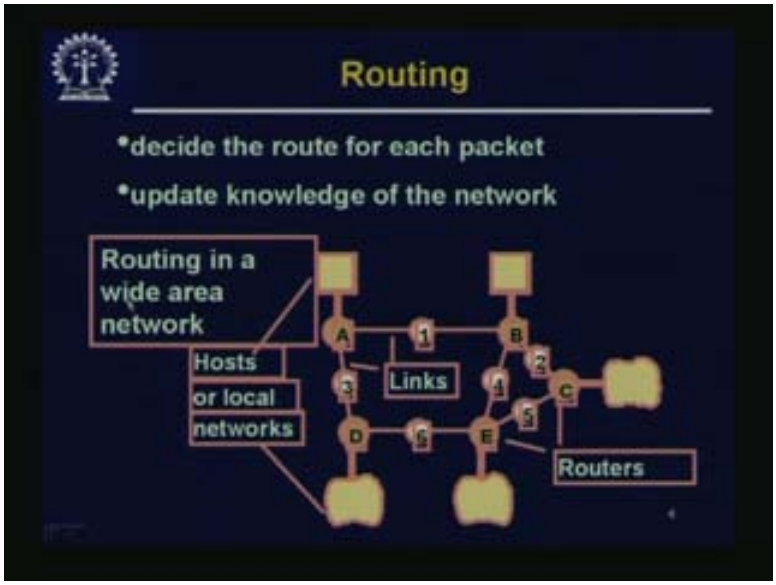
Suppose you have a host or LANs connected to some routers say A, B, C, D, E and then through the links 1, 2, 3, 4, 5 and 6 respectively then for example when the router A gets a packet from a local network which is connected to it which may be destined for the LAN which is connected to router C. So it has to decide whether to take link 1 or link 3. Obviously it does not take this link because this is where it is coming from and obviously it is destined to some other sort of remote so it has to decide. Although in this particular example you may theoretically reach C both by taking link 1 and link 3 but then these links may be of different quality, May be something like A, D, B,C, E is a bit of choice.

(Refer Slide Time: 11:31- 12:12 min)



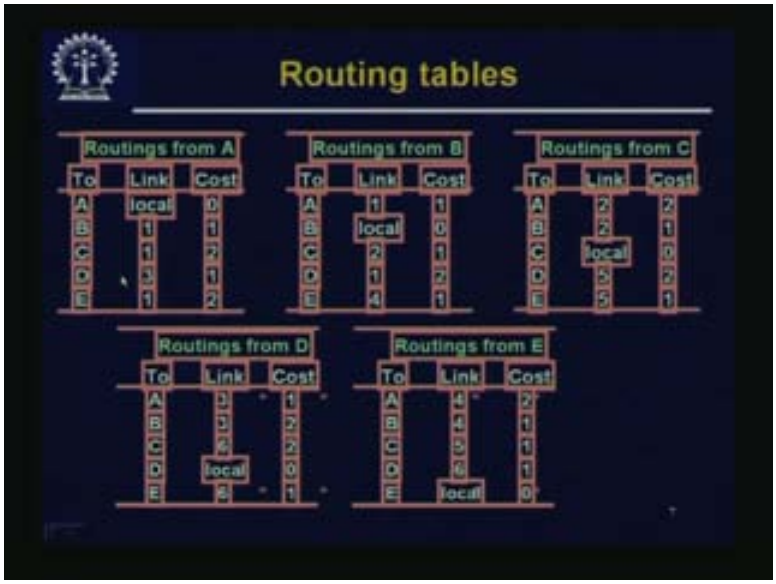
As mentioned earlier these are the routing tables. We have the routing tables in routers. They look somewhat like this. For example, let us look at the routing from A and this may be just one form of it. It may not be exactly used in this form but let us look at it. Suppose you want to route to the router A which is again local because we are sitting on router A, for B you take link 1, for router C link 1, for router D link 3 and for router E link 1.

(Refer Slide Time: 12:13- 12:24 min)



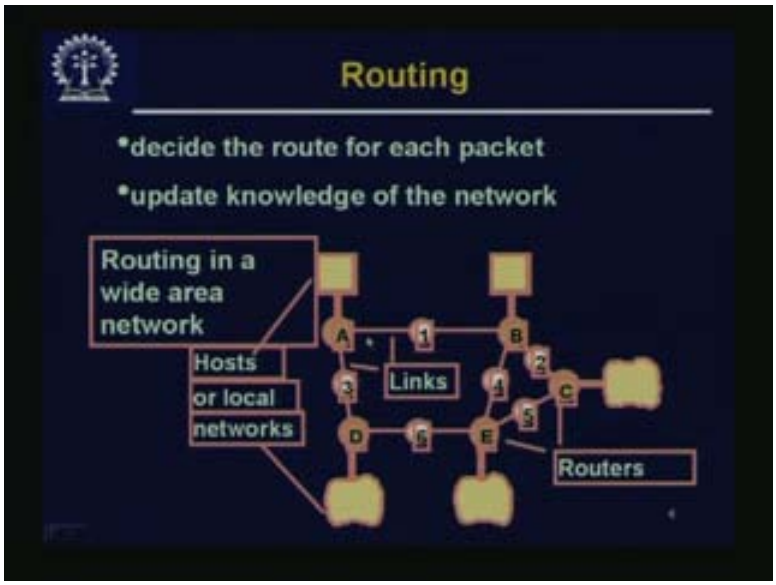
From A to B is link 1, may be C is also link 1 and D is link 3 and E is again link 1 and so on.

(Refer Slide Time: 12:25 - 12:59)



Similarly, B will have a routing table and C will have a routing table and so on. Suppose you take any destination A, now for A let us consider a tree with a root at A. Now B connects to A through link 1 and C connects to A through link 2. Obviously link 2 is not taking C directly to A but link 2 is only taking C to B but that is the preferred path for connection from C to A.

(Refer Slide Time: 13:00 - 15:41)



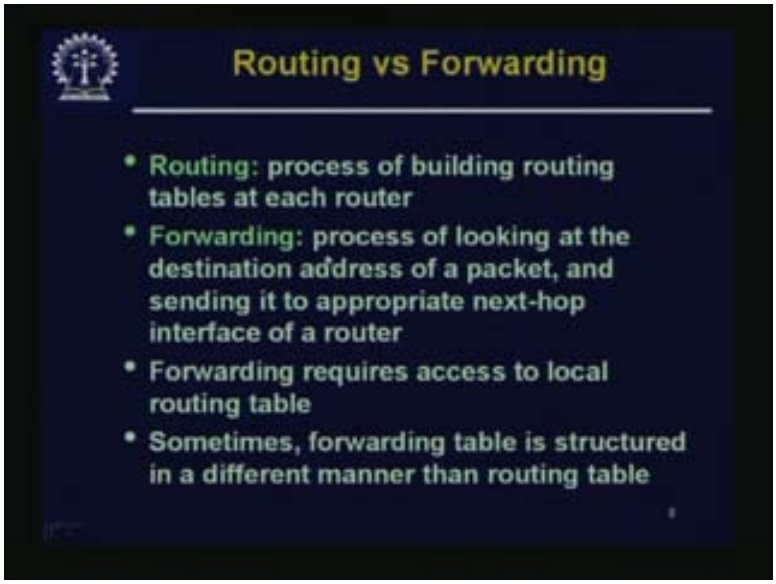
If you think about it this way, for each destination we have got some kind of a tree if the network was very bigger. Here the network is very small so the tree is only two levels deep. But the tree could be very deep may be 10 or 15 levels deep. So for each destination we actually have a tree which is implicit in these routing tables which are

distributed. At each node we try to see the local link to be taken for that particular destination.

As I said, the local link may not take you directly to the ultimate destination. But the local link will take you somewhere and that particular node will again have a link for the same destination. This way, if everything is working fine, after some hops you will reach the final destination. This means that some of the other nodes may be directly connected, some may be 2 hops away, some may be 3 hops away etc. But overall there is an implicit tree for each destination. And for one movable link of this tree is in one particular link of this routing table just according to the destination.

In other words, if there are n nodes and there are n implicit trees and these n implicit trees are distributed over n nodes. So it is one link from each tree in the routing table of a particular node. In that way you have a routing table of size n including the root which is the local link. And somehow you need to maintain this tree and that is the job of a routing protocol. Later on we will see different routing protocols and also see how these implicit trees may be maintained or rather how these routing tables have to be maintained.

(Refer Slide Time: 15:42- 16:44 min)

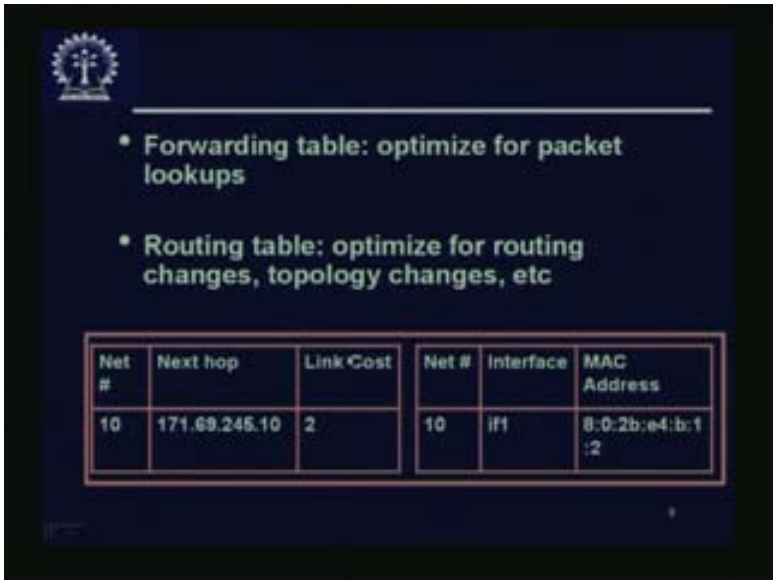


When there is a routing table there is a question of forwarding. Routing is the process of building routing tables at each router. Forwarding is the process of looking at the destination address of a packet and sending it to appropriate next hop interface of a router. This means, once through a routing protocol you have a routing table then a packet actually arrives and you have to forward it to the correct interface of that router. So, you look up to this table and the interface to which the packet must be sent and forward it. So this routing or forwarding are two different and distinct parts of the router.

Actually sometimes these two are diverged even more. For the time being we assume that routing and forwarding happen at the same place and the routing table itself is being used

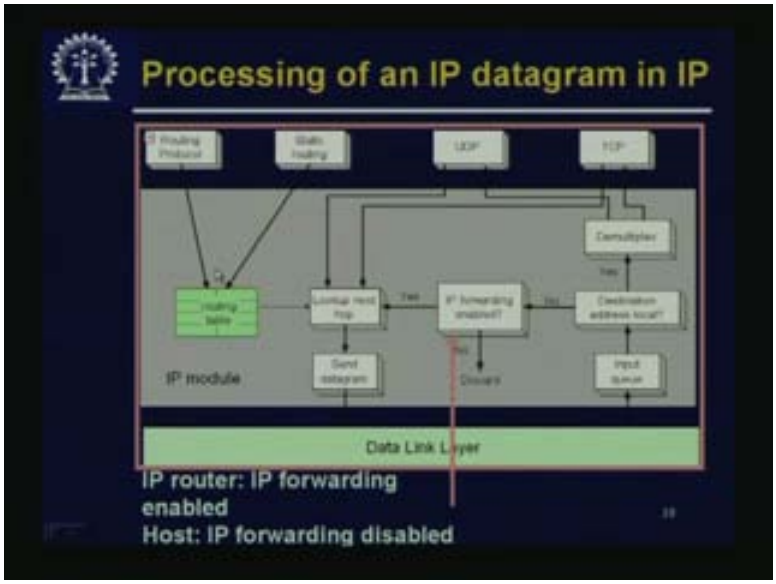
for forwarding although that may not always be the case. Forwarding requires access to local routing table. Sometimes forwarding table is structured in a different manner than routing tables. So forwarding table is optimized for packet look ups. Routing table is optimized for routing changes, topology changes etc.

(Refer Slide Time: 16:45 - 18:05 min)



A routing table may look like this: say, for net number 10 the next hop would be this IP number because the routing table is working in the IP address. This IP address is version four addresses and it contains four numbers all less than 256 so it is 171.69.245.10. The link cost may be there. In forwarding, we really do not care what the IP address or the next hop is. We do not even care about the link cost because all these are a part of setting up the routing table. In the forwarding table we just wanted to know the interface as to what is the local interface to which this packet has to be sent and what is the MAC address at the next hop. This is what we are more interested in. Basically you can just add your data-link headers and just send it over to the physical layer. This is a slightly higher level and the abstract view of processing an IP datagram.

(Refer Slide Time: 18:06- 21:09 min)



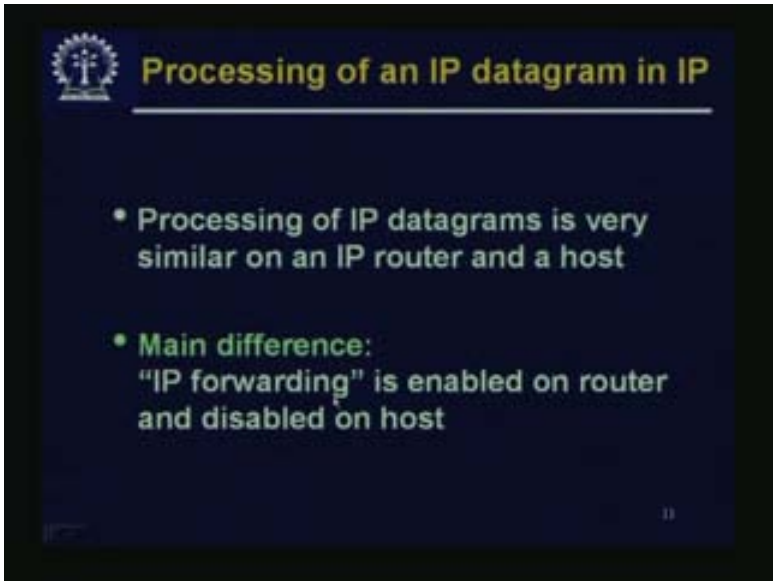
In this IP module there is a routing table which is the central thing. There is a routing protocol which makes this table. Sometimes we also use static routing, for the time being let us consider that it has been manually configured. Some of the entries may have come through a routing protocol while some of the entries may have been manually configured. Now, when a packet comes from an upper layer it will come from some transmission layer protocol.

Two of the most common transmission layer protocols are TCP and UDP. We will see what they are later on. But let us assume that some packet has come through UDP with some destination IP address in it. You look up at the routing table, the next hop and send the datagram. Or the same thing must have come through TCP also.

When we are discussing the processing of the IP datagram in the IP layer the IP layer is present in two different places. In one place it is the regular host the PC and in the other place it is a router. The jobs of the two places are a little different. If a packet comes from outside to a PC, and is not meant for the PC, the PC is simply going to drop that packet.

In the case of a router, if a packet comes from outside, it looks up the destination and then actually forward it. So in a PC the forwarding table may be disabled whereas in a router the forwarding table will be enabled. If the packet originates from machine PC itself then it has to go out on its way. It will send the packet to the router. The IP datagram it is sent to the network layer. This is a high level view of what is happening in the IP datagram processing.

(Refer Slide Time: 21:10 - 21:21 min)

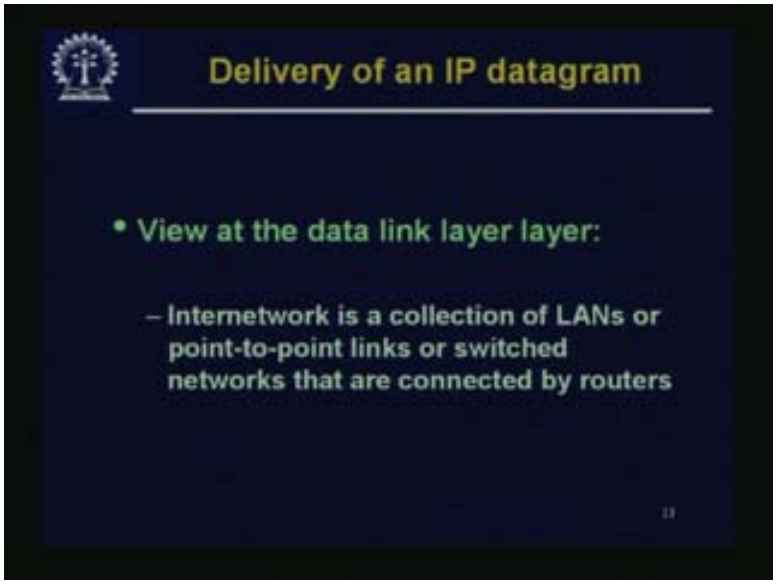


The processing of IP datagrams is very similar on an IP router and a host. The main difference is IP forwarding is enabled on router and disabled on host.

(Refer Slide Time: 21:22 - 21:45 min)

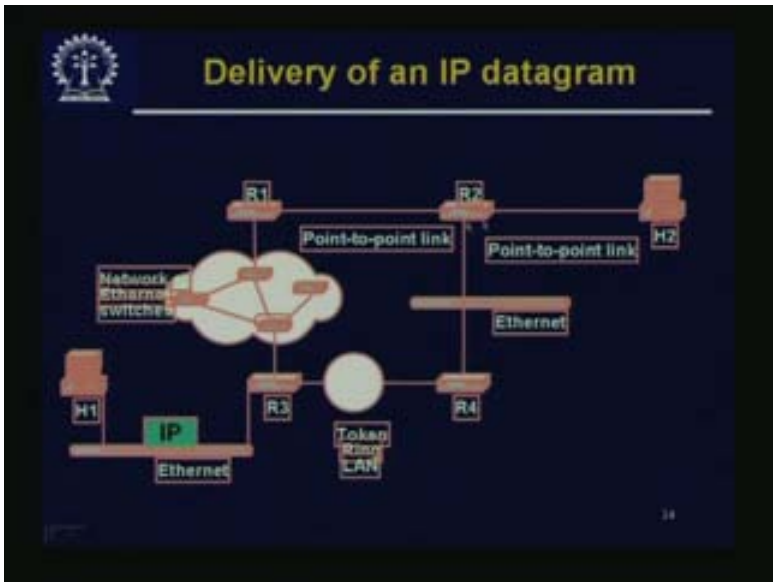
Now when the IP forwarding is enabled, if a datagram is received but it is not for the local system, the datagram will be sent to a different system. When IP forwarding is disabled, if a datagram is received it is not for the local system and the datagram will usually be ignored.

(Refer Slide Time: 21:46 - 22:03 min)



The view at the data link layer is somewhat different. Internetwork is a collection of LANs or point-to-point links or switched networks that are connected by routers. So this is the data link layer view of the IP datagram.

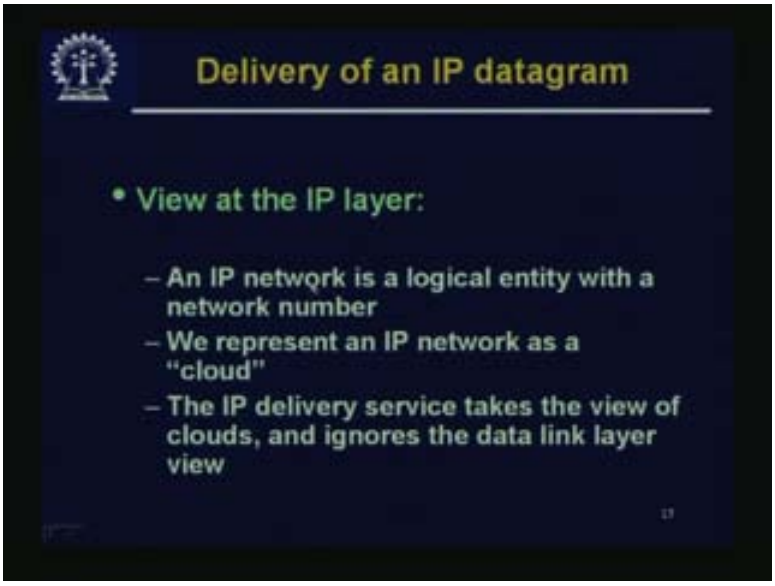
(Refer Slide Time: 22:04 - 23:02 min)



In this diagram there may be some point-to-point links or some LANs, etc. and they are all connected by some routers R1, R2, R3, R4 etc. A particular host places an IP datagram on the local ethernet that is destined for outside it will eventually reach the local router and the router will decide whether to give it to another network such as the network of Ethernet switches, token ring etc. Through different networks the packet proceeds through the routers to this. When you look at it from a data link layer point of

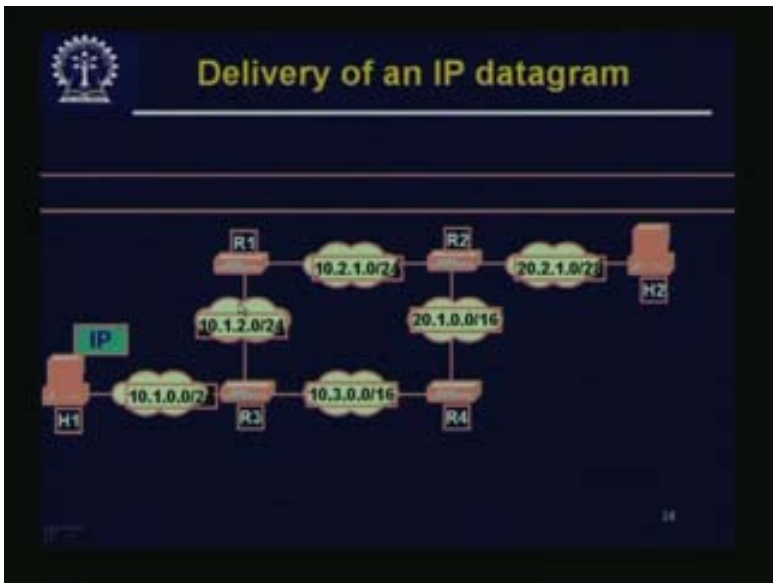
view all these switches become visible whereas at the IP layer only the routers and the networks will be of main concern.

(Refer Slide Time: 23:03 -23:26min)



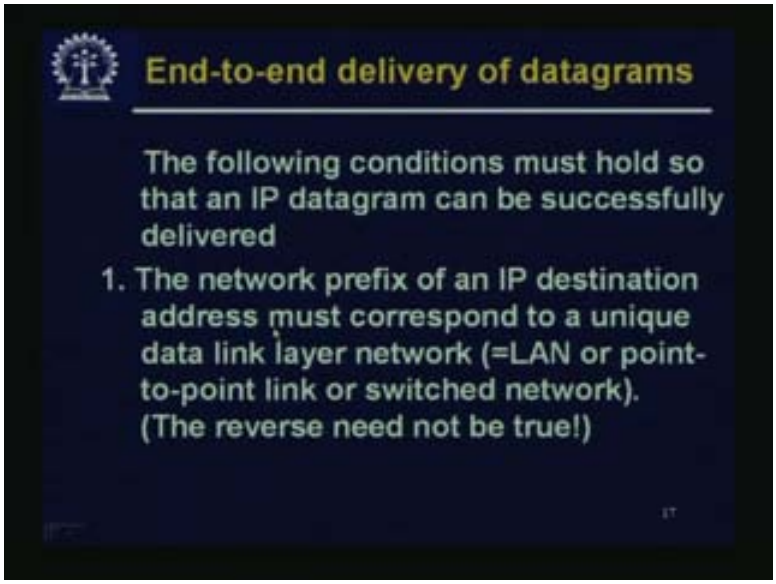
A view at the IP layer: An IP network is a logical entity with a network number. We represent an IP network as a cloud. The IP delivery service takes the view of clouds and ignores the data link layer view. That means the details of these actual switches etc are in the data link layer view whereas in the IP layer view it will simply be a cloud.

(Refer Slide Time: 23:27 - 23:26 min)



In this picture there are routers R1, R2, R3, R4, etc and the connecting networks are shown as clouds. Each network has some number.

(Refer Slide Time: 23:47 -27:13min)

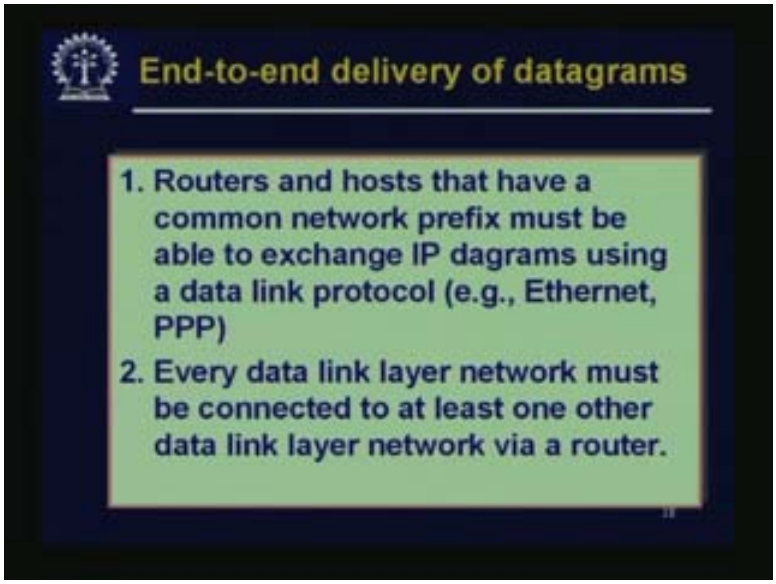


The following conditions must hold so that an IP datagram can be successfully delivered. The network prefix of an IP destination address must correspond to a unique data link layer network which is equal to LAN or point-to-point link or switched network. The reverse need not be true. This is quite fundamental. You have already seen examples of IP addresses. They are basically four numbers each less than 255 that is something like 144.16.192.53. This may be the IP address of a particular machine. In the network layer it is not possible to handle all the machines individually because that will make the problem really big.

Therefore, as our first step in reduction or scaling, actually in the remote routers we do not usually keep track of the specific IP addresses of specific machines. We just keep track of how to go to that network which contains this IP address. So the IP address usually has two parts: the leading part that is the first few bits or bytes is a address of the network whereas the last few bits or bytes may be reserved for a particular machine within that network. This is how a global IP addressing scheme is. This is not as neat as in telephone numbering which exactly tells you the particular state, area, LECA and the particular exchange finally so it is not that neat. But at least the first few bits or bytes will be associated with all the IP addresses in a particular network. If you just take that prefix part you know that it precisely means that particular network and no other network will have the same exact prefix.

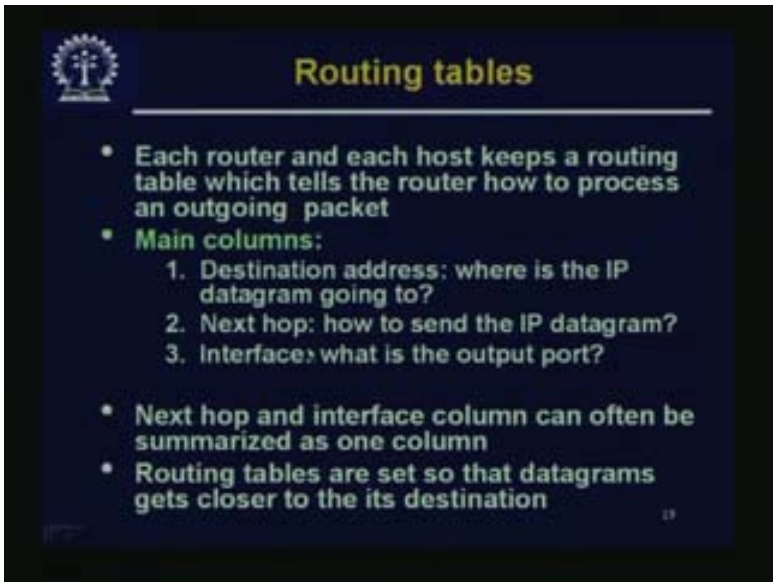
The network addresses have to be globally unique because now-a-days our network is really span the entire globe. Therefore this is called as the network prefix of an IP destination address and this must correspond to a unique data link layer network. But the reverse need not be true which means one data link layer network may have two different network prefixes.

(Refer Slide Time: 27:14 - 27:37 min)



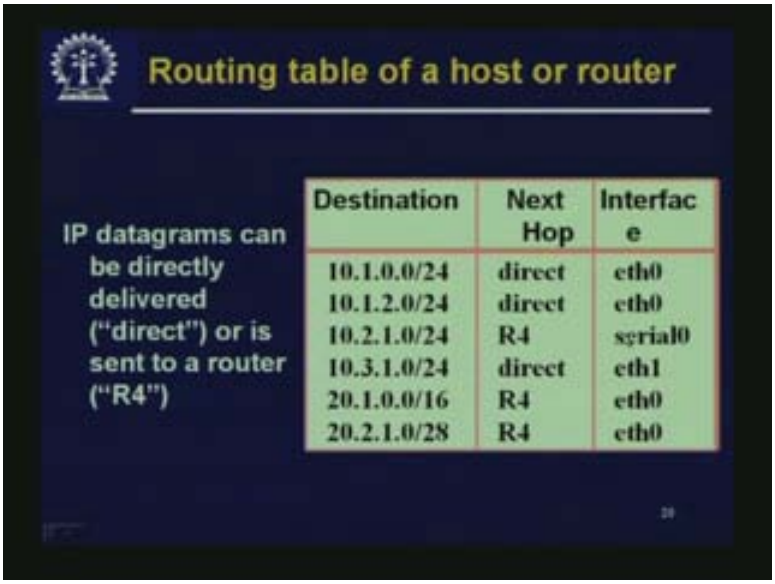
So routers and hosts that have a common network prefix must be able to exchange IP datagrams using a data link layer protocol such as Ethernet, PPP etc. Every data link layer network must be connected to at least one other data link layer network via a router.

(Refer Slide Time: 27:38 -28:08 min)



Each router and host keeps a routing table which tells the router how to process an outgoing packet. The main columns as we have already seen are (1) the destination addresses, i.e. where is the IP data gram going to, (2) next hop, or how to send the IP datagram and (3) interface or what is the output port. Next hop and interface columns can often be summarized as one column and routing tables are set so that the datagram gets closer to it is destination.

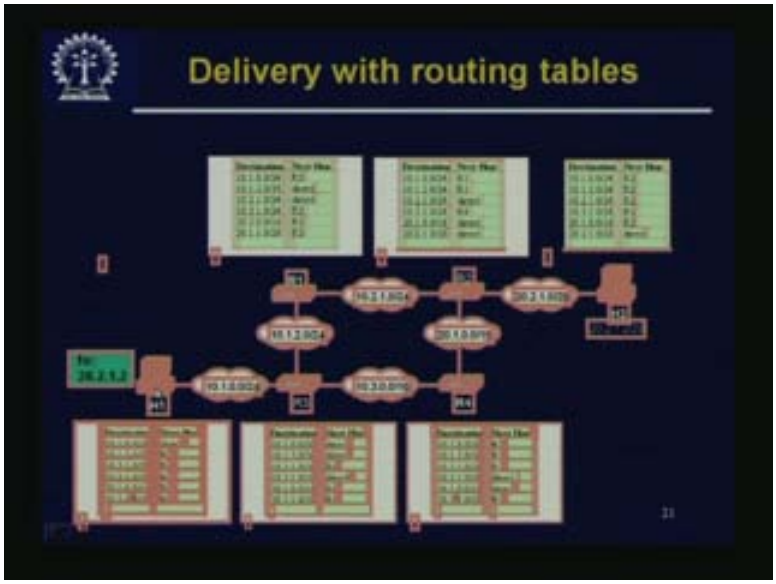
(Refer Slide Time: 28:09 -29:39 min)



This is another example of a routing table. IP datagrams can be directly delivered which means these are in the local network. Therefore they go through the interface called Ethernet zero whereas these addresses are outside so this one had to go through a router or to a point-to-point link. Or this can be some other network altogether. Now the prefix has distinctly changed.

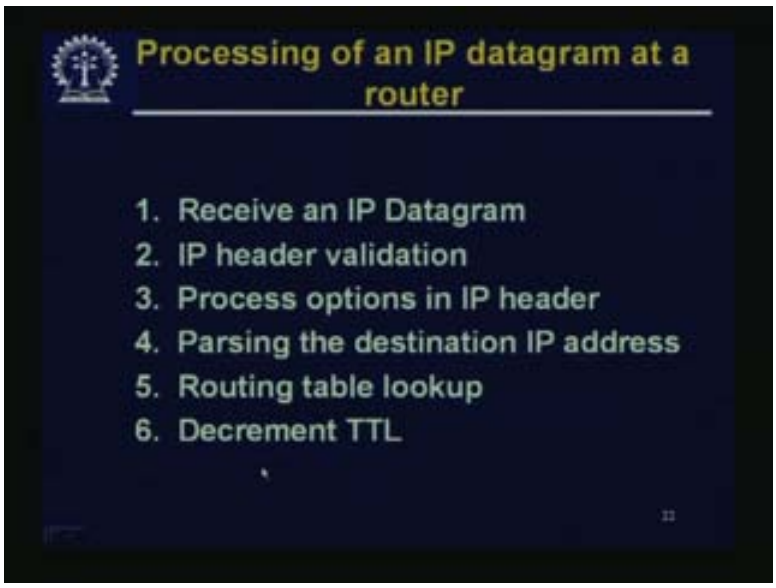
For example, 10.1.0.0/24 means any number from 0 to 24 can be there. So, for all these IP addresses, you just deliver the datagrams directly. Similarly 10.1.0.2 is also connected directly which means they are all in the same network. And then there is a point-to-point connection through a serial link on this router which is also may be very closely connected to the same set of networks. There may be other networks out in the WAN which really starts from 20. So, for those networks you again have to go to the router and go out through some port of that router.

(Refer Slide Time: 29:40 -30:22 min)



If you take a more global view these different routers will be having routing tables. We know the details of these routing tables and what they contain and this is how one particular IP packet which originates here will go to a router then to a next router and then to another router and so on.

(Refer Slide Time: 30:23 -33:41 min)



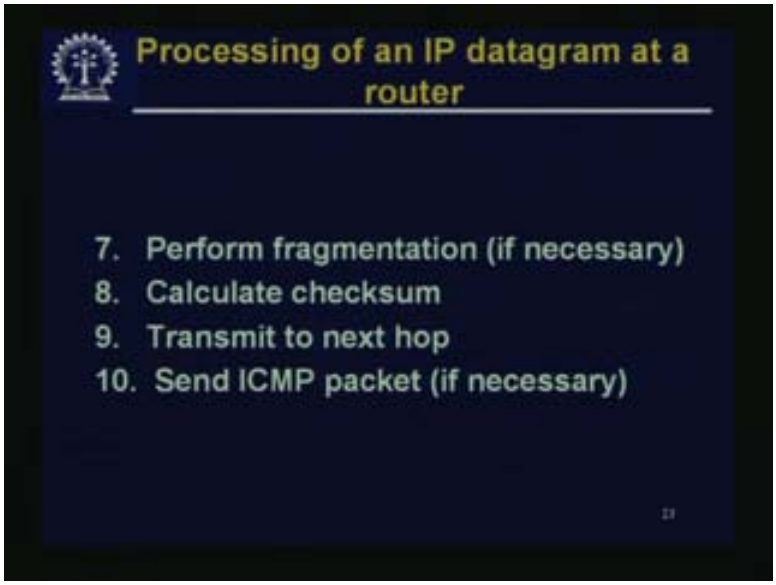
Processing of an IP datagram at the router:
First we have to receive an IP datagram then IP header validation. The IP protocol is a network layer protocol. Previously we discussed about a lot of data link layer protocols but now we are talking about IP protocols. And for these IP protocols once again you require some information to be exchanged between peers. This information will be in the header called the IP header because in the network layer we are mainly concerned with IP

so it is the IP header. In any case the IP header has to be validated. If there are some options in the IP header they have to be processed. The destination IP address is parsed from this header. Then we do a routing table look up and we decrement TTL i.e. we decrement time to leave.

Here is a common example. In this distributed fashion we are trying to capture a good and consistent and correct picture of the entire global connectivity which gives you the best connection. But in practice this may not always be possible because the global picture may change from time to time. So, to get the entire global picture in a very correct fashion is not possible sometimes. You may have inconsistent routing table entries and that may lead to various things such that it may lead to a loop in the routing table. The loop may not be in one routing table but if you take several routing tables together then you can see that the packet will go in a loop.

Once a packet starts going in a loop it will continue in that loop because each time it comes to the router the router will see its own routing table locally and send it to the next one which was hopefully in a correct path. But actually now it is in the vicious ring so this packet will just go on circulating ad infinitum. To stop this we put some kind of restriction on the number of hops a packet will take may be 30. Each time an intermediate router forwards a packet it will decrement this time to leave that is from 30 to 29 and from 29 to 28 and so on. After 30 hops whichever router finds a packet with a TTL zero will simply drop the packet either that packet is going in a loop or the packets have gone very astray because of mistaken entries in the routing table and so on then perform fragmentation (if necessary).

(Refer Slide Time: 33:42 -35:18 min)



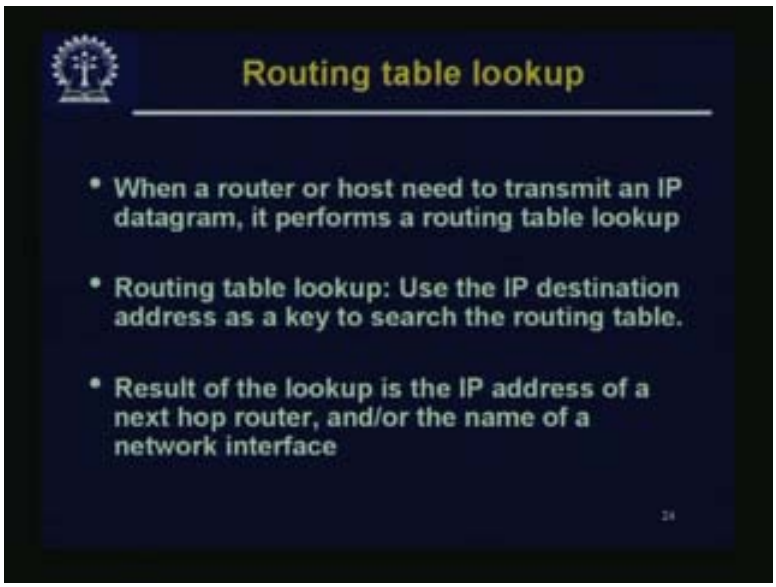
We will see the details of fragmentation later on. Fragmentation here is, what you are doing is that you are going from one network to another network to another network and so on. All these different networks are on different administrative controls and different domains and they may even have different data link layer technologies. Some token ring

may be connected to some Ethernet and there can be all different kinds of networks in between.

Now, suppose the source had sent an IP packet which was quite large but inside one particular network it is not possible to handle such a large packet. It would be unfortunate if you drop the packet all the time because it will never go through. Therefore what is done is that this big packet is broken up into small fragments and the fragments are sent. Later on when you are in a sort of wider area the fragments are again reassembled into a big packet and sent along when it reaches the destination. Then you calculate the check sum which is of error in connection as we note and transmit to the next hop and send an ICMP packet if necessary.

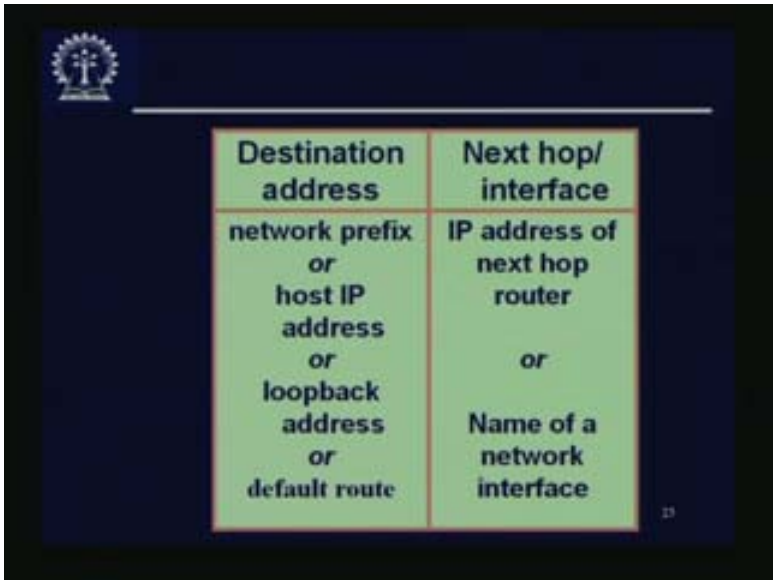
ICMP stands for Internet Control Message Protocol. The routers may use ICMP packets for communicating between each other and sending various messages if necessary. We will see one example list now and the rest later.

(Refer Slide Time: 35:19 -35:41 min)



When a router or host needs to transmit an IP datagram it performs a routing table lookup. So, use the IP destination address as a key to search the routing table. The result of the lookup is the IP address of the next hop of the router and/or the name of the network interface. We have seen that.

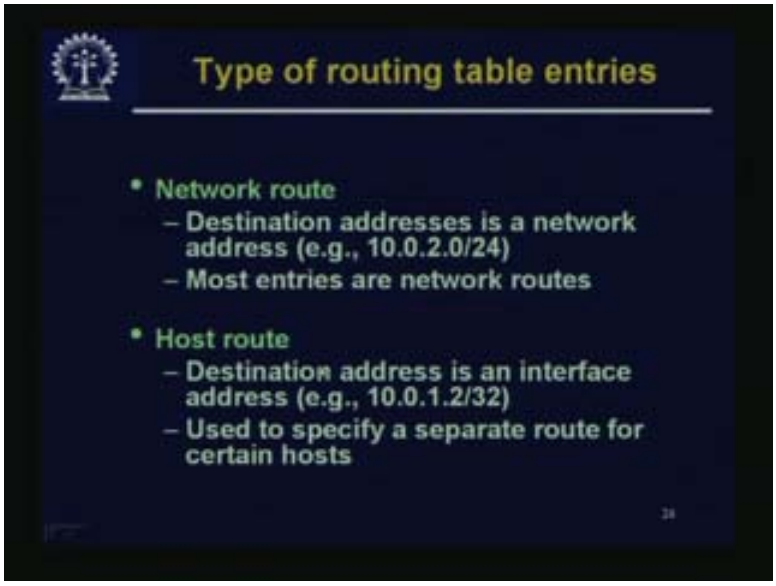
(Refer Slide Time: 35:42 - 37:09 min)



Therefore either you take the network prefix or host IP address or loopback address or the default route. Loopback address means this is meant for local consumption so it will go back to the same machine. So it is coming down from a machine and it contains a loopback address then it goes back to the same machine. Why would somebody want to send the packet like this? One process of the packet of the host is sending some packet to another process in the same host and it is using this network operating system part for sending that message.

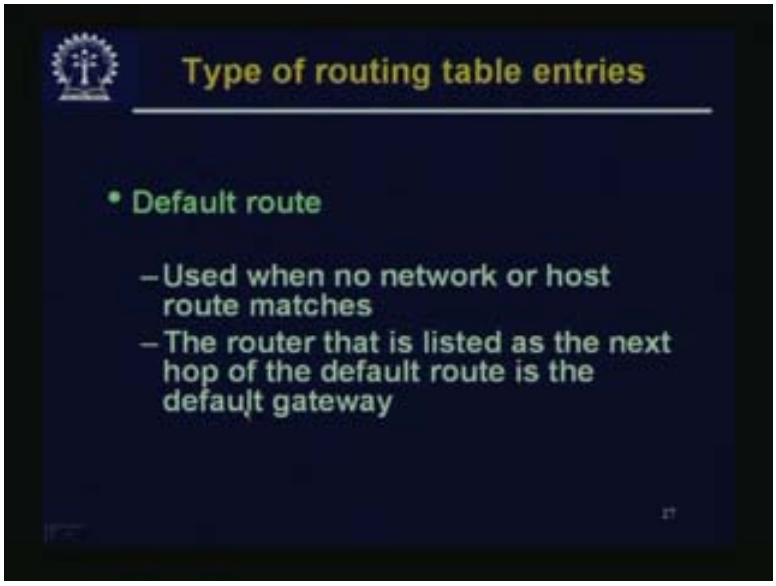
Default route is very important because you cannot keep the network prefix for all possible networks in the world in this table then this table will then become very large. So you will have fewer entries for the network prefixes and if your network is something else may be there is a bigger router somewhere that knows about all these networks. So there is a router which is likely to know about this particular network prefix which has come so you send it to a default route. And on this side you have the IP address or the name of the network interface.

(Refer Slide Time: 37:10 - 37:26 min)



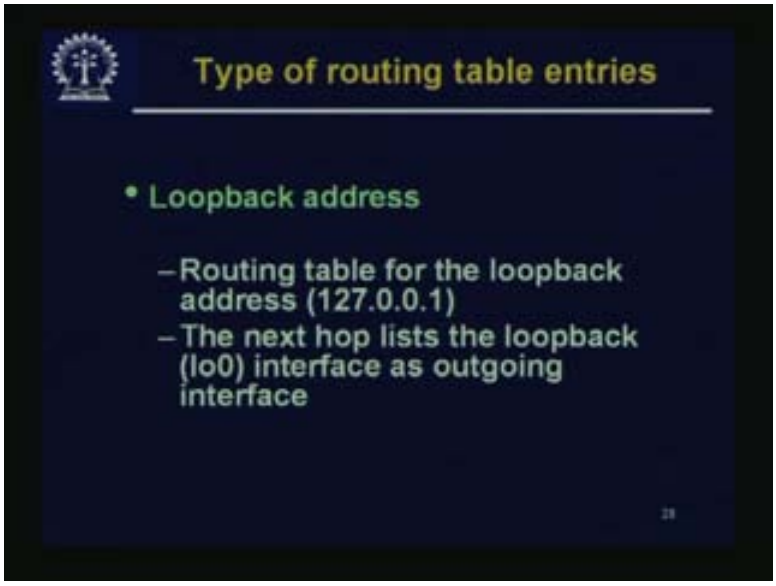
So the destination address is a network address, most entries are network routes. For the host route the destination address is an interface address which is used to specify a separate route for certain hosts.

(Refer Slide Time: 37:27 - 38:09 min)



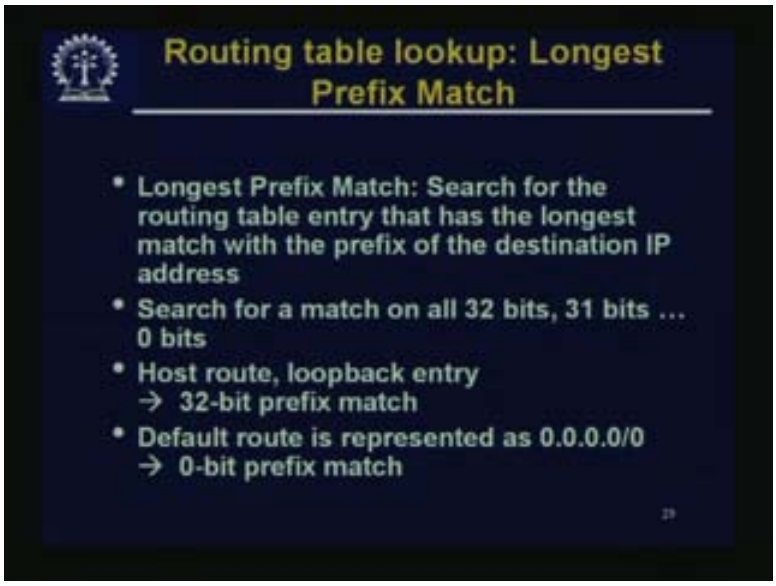
The default route is used when no network or host route matches. The router that is listed as the next hop of the default route is the default gateway. We are calling it gateway because this is not a packet for a network which is close by. This is a packet for some arbitrary distant destination, this is a smaller router that is connected which will send it to the gateway and the gateway will in turn send it to a bigger router to find its final destination.

(Refer Slide Time: 38:10 - 38:27 min)



Loopback address:
Routing table for the loopback address is the particular loopback address which is used in IP which is 127.0.0.1 and this is meant for local consumption. The next hop lists and loopback interface as outgoing interface.

(Refer Slide Time: 38:28 - 40:04 min)



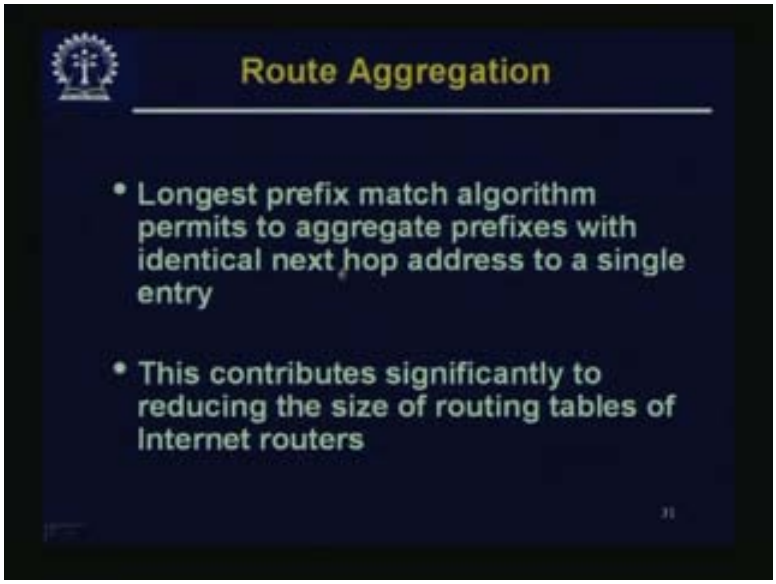
To minimize the size of the routing table we use the longest prefix match, i.e. we search for the routing table entry that has the longest match with the prefix of the destination IP address. It means search for a match on all 32 bits. The IP address contains four integers less than 256 i.e. four bytes which is actually 32 bits. So an IP address in IPv4 address is 32 bit long. So first you try to match all the 32 bits with some entry in the table.

If the 32 bit does not match then you take only 31 bits and check whether they match and you keep on doing it and keep on reducing till you get a match so you have identified the first entry that matches with the longest prefix where such a match is possible. The host route loopback entry is a 32 bit prefix match. The default route is represented as all zeros which is a zero bit prefix match. That means there is a zero entry which will give you the next hop as the gateway because now it has not matched with anything. Finally this is a zero bit prefix match.

(Refer Slide Time: 40:05 - 41:14 min)

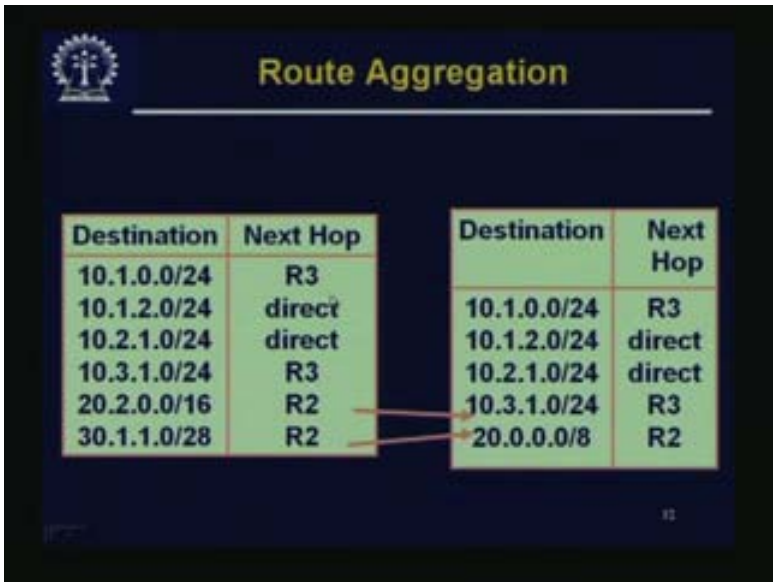
Suppose the destination address that has come in is 128.143.71.21 then of course the 128 and 143 parts have matched with this but then here this is zero and this is 71 so this is a much better match here with the one shown in red. Similarly, 128.143.71 is also matching here but the next number is 21 which will match better with this rather than with this range. This is where the match will take place and you will send to router R4. The default router at the gateway is shown as R5. So the longest prefix match for this is for 24 bits with entry. You can find this out if you actually break up 21 into its binary form and see how many bits are matching but this is matching with the 24 bits etc, so data gram will be sent to R4.

(Refer Slide Time: 41:15 - 41:32 min)



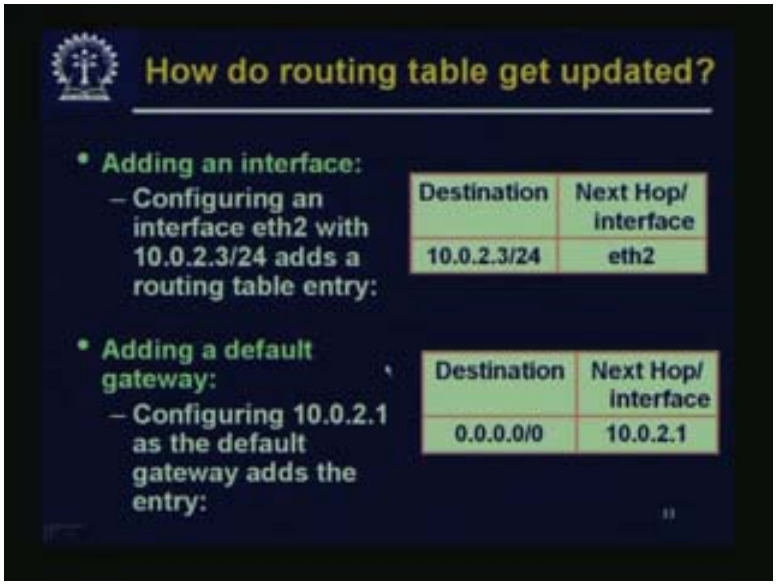
The longest prefix match algorithm permits to aggregate prefixes with identical next hop address to a single entry. This contributes to significantly reducing the size of the routing tables for internet routers.

(Refer Slide Time: 41:33 - 42:31 min)



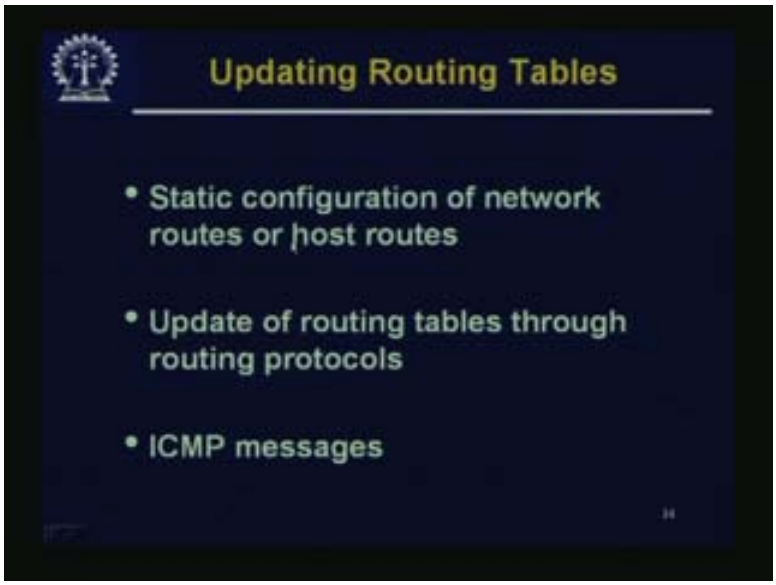
Suppose for 20.2.0.0 to 16 I would have gone to router R2 and for 30.1.1.0 to 28 I would have gone to R2 once again. Now we see that the next hop is the same and what we can do is, instead of 20 and 30 if we make the entry as 20.0.0.0/8 and put it as R2 then because of longest prefix match then whenever something also comes in this range it will have a longest prefix match with this rather than with this because this is taken over here and 30 is naturally closer to 20. So instead of two entries we keep only one entry in the routing table which helps in reducing the size of the routing table.

(Refer Slide Time: 42:32 - 42:56 min)



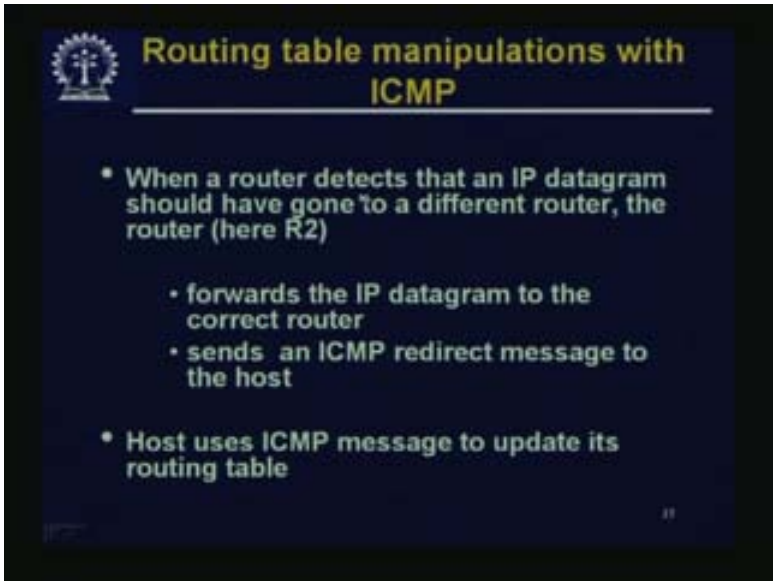
How do routing tables get updated? One way is to add an interface and then configure the same so it adds a routing table entry. This is manual configuration. We can also add a default gateway that means for the destination that is the default route we can add a gateway. This is once again a manual updating.

(Refer Slide Time: 42:57 - 43:32 min)



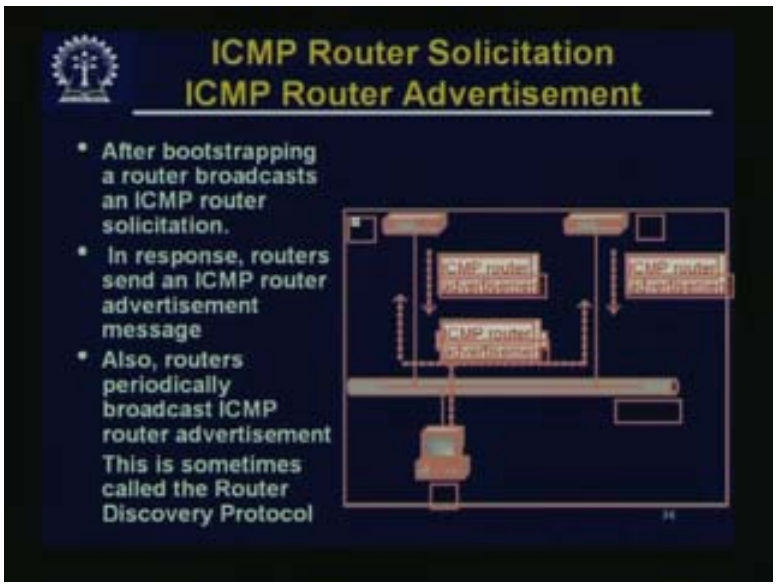
So it is the static configuration of network routes or host routes. If some particular route is forced then I might put in a static configuration of what they are. Routing tables also get updated through routing protocols. There may be ICMP messages from some router which may update the routing tables. So these are the different ways in which a routing table may get updated.

(Refer Slide Time: 43:33 - 44:31 min)



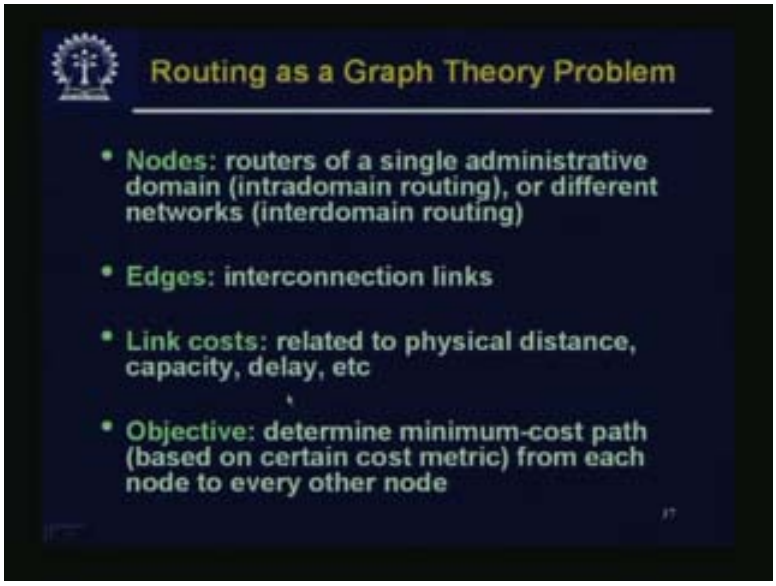
For example, for this ICMP when a router detects that an IP datagram should have gone to a different router the router (here R2) forwards the IP datagram to the correct router and sends an ICMP redirect message to the host. The host uses the ICMP message to update its routing table. What is happening is that one particular host had sent the IP datagram to one router. Now this router sees that it need not get it from this host and that host should have sent it to that router. This router will now send it to the that router anyway and send an ICMP message to this host saying that from next time onwards when you have got this destination please send it to that particular router rather than sending it to this destination. This is one example of how ICMP may be used. These are the different kinds of ICMP messages.

(Refer Slide Time: 44:32 - 45:46 min)



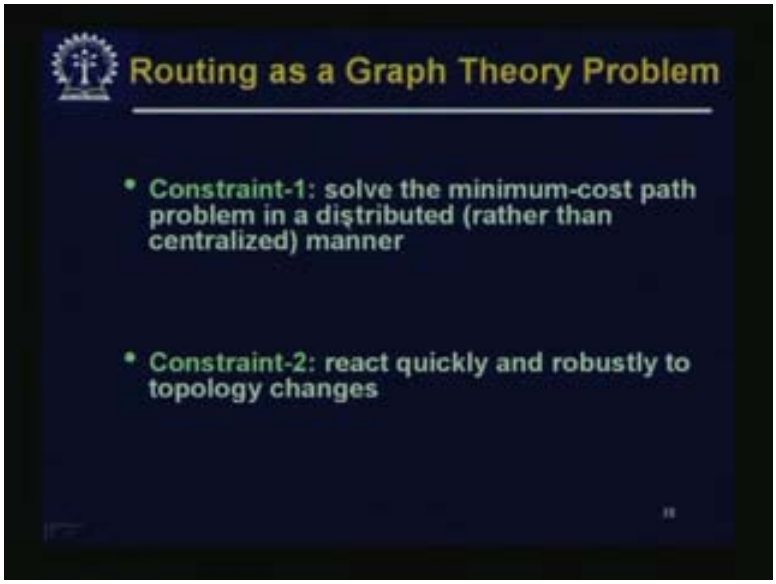
The other thing is ICMP router solicitation and ICMP router advertisement. When a router is switched on for the first time how will other routers know that this router has come up? Since the other routers do not know about the existence of the new router which has come up it is was not sending any message to it. So, after bootstrapping a router broadcasts an ICMP router solicitation. It sends an ICMP and advertises itself and solicits ICMP messages from the neighboring routers. In response the router sends an ICMP router advertisement message. Also, routers periodically broadcast ICMP router advertisement. This is sometimes called Router Discovery Protocol. This has to be done periodically because some router may have gone dead in the meanwhile. Therefore by doing things periodically you try to keep it as current as possible.

(Refer Slide Time: 45:47 - 46:28 min)



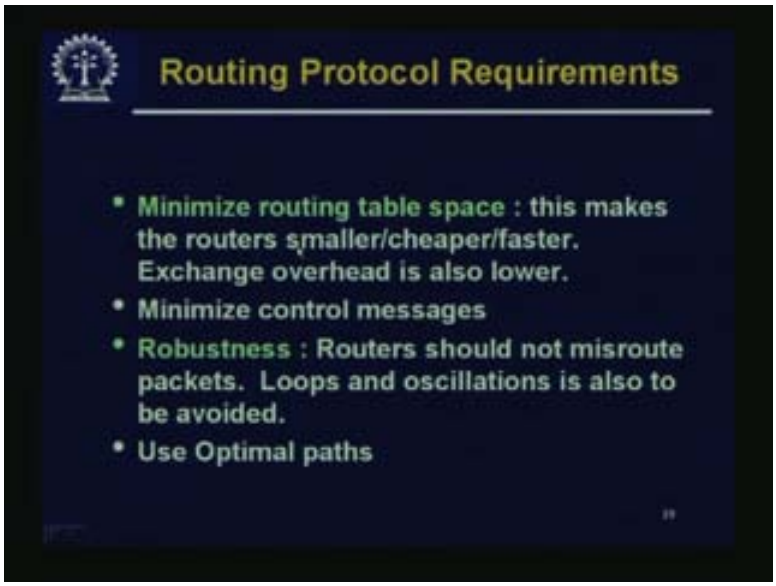
We can look at routing as some kind of a graph theory problem where (a) the nodes are the routers of a single administrative domain or different networks, (b) the edges are interconnection links, (c) link costs are related to physical distance, capacity, delay, etc and (d) the objective is to determine minimum cost path. You can formulate it as a graph theory problem and this particular graph theory problem can be handled in different ways. We will see two different ways later on.

(Refer Slide Time: 46:29 - 46:41 min)



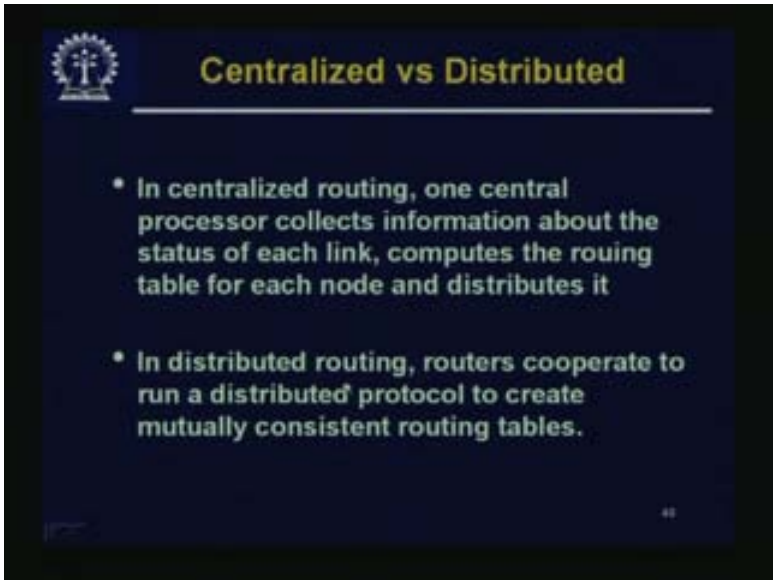
The problem has some constraints, one is to solve the minimum cost path problem in a distributed manner rather than centralized manner and constraint two is to react quickly and robustly to topology changes.

(Refer Slide Time: 46:42 - 47:26 min)



There are routing protocol requirements. One is to minimize routing table space, i.e. with all these millions of networks working at the same time minimizing the routing table space is always very important. This makes the routers smaller or cheaper or faster, minimizing or controlling messages is also important. Routers should be robust and not misroute packets. Loops and oscillations must also be avoided. Finally optimal paths must be used. All these are different routing requirements. It is not that we can get 100% of the requirements all the time but we try to do it as best as we can.

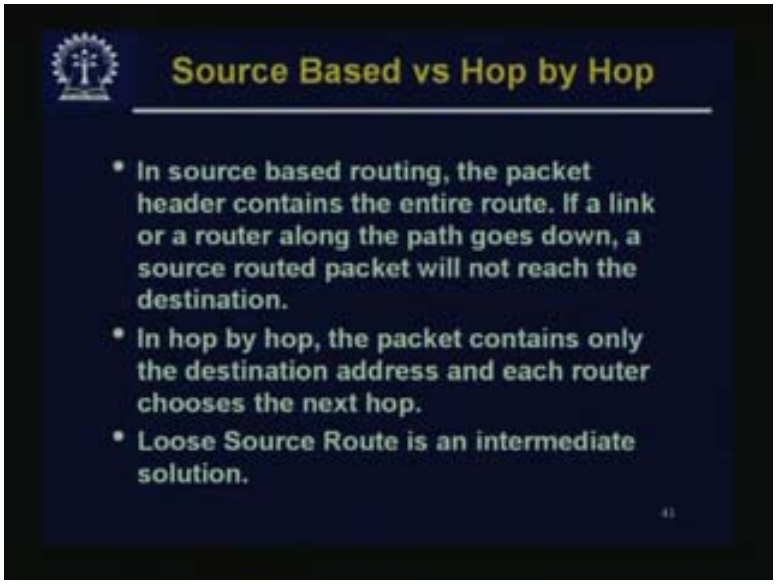
(Refer Slide Time: 47:27 - 48:40 min)



Now we will quickly go through the different approaches to routing. One is the centralized versus distributed approach. In centralized routing one central processor collects information about the status of each link, computes the routing table for each node and distributes it. This is possible only in a small number of cases and not all the time.

Obviously it is not possible over the entire internet because there is no such centralized routing that would handle the scale. In distributed routing, routers cooperate to run a distributed protocol to create mutually consistent routing tables. In distributed routing also there may be two approaches. One is that you distribute the local information only and then globally try to come to a solution. The other is that you distribute the information globally and then locally you simply route some kind of a centralized algorithm to know because you have now got the global picture in each of the places.

(Refer Slide Time: 48:41 - 49:53 min)

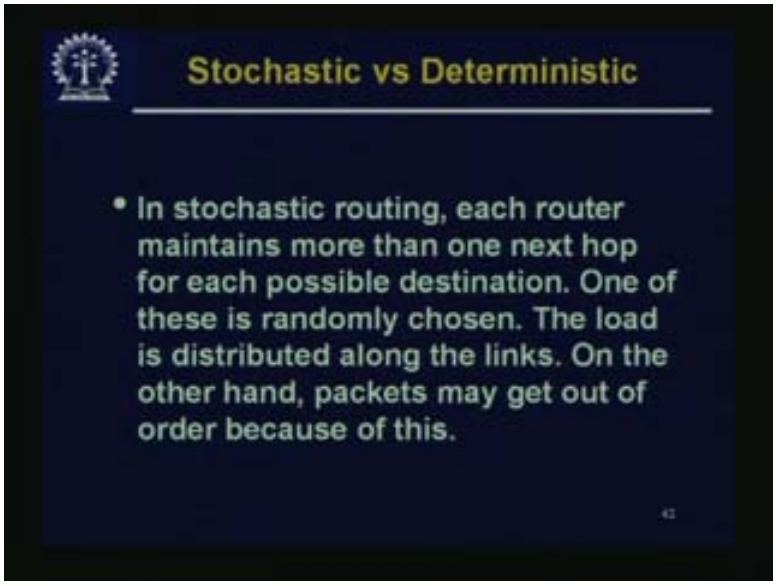


Routing may be source based or versus hop by hop. In source based routing the packet header contains the entire route. If a link or a router along the path goes down a source routed packet will not reach the destination because the route has been fixed by the source. The intermediate routers do not do anything. If the next hop is available it will send the packet otherwise it will drop it.

In hop by hop routing the packet contains only the destination address and each router will consult its own routing table and find out what is the next hop and then choose that next hop. But in the source routing the route is fixed from the beginning.

Loose source route is something in between, it is an intermediate solution. In loose source route what is done is that instead of specifying the entire path you specify some sort of islands in between. That means you go from one router to the next through several hops then again several hops and so on. So this is something intermediate between strict source routing and pure hop by hop routing.

(Refer Slide Time: 49:54 - 52:47 min)



Routing may be stochastic or deterministic. In stochastic routing each router maintains more than one next hop for each possible destination. One of these is randomly chosen. So the idea is to distribute the load evenly along the links. On the other hand, packets may get out of order because of this. It is because the packets from the same source travels to the same destination and the first packet may be stochastically chosen to go through this path and another may be stochastically chosen to go through this path. The probability of choosing either this path or that path can be based on some metric like the delay. But in the end the packets may reach out of order.

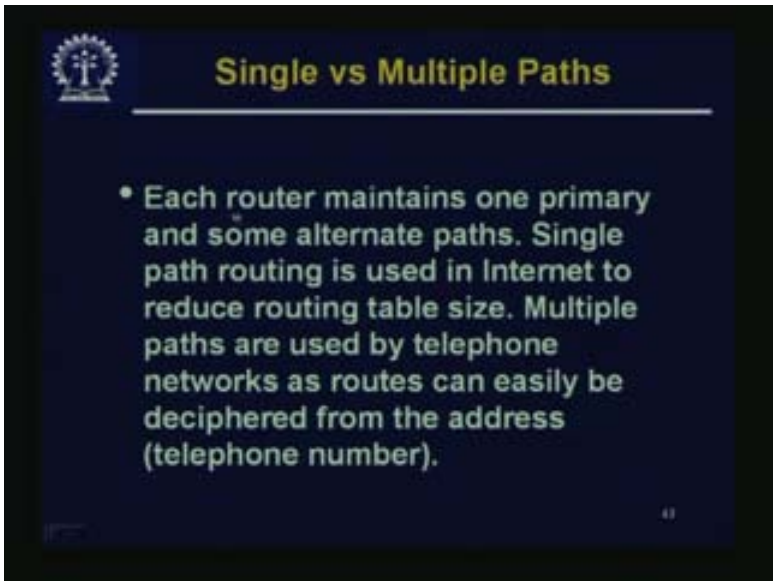
Please remember, the service the network layer is providing is just to send the packet from one end to the other part of the network. Here this part has been said explicitly but it is also important to understand what has not been said. It has not been said that this service is going to be very reliable which means that in the interim some router may drop a packet so your packet may not reach the destination at all. So reliability is not guaranteed.

Another thing that has not been said is that all the packets you sent from destination A to B will reach the other end in the same order in which they were sent. The first packet may reach later than the second packet because may be it came through two different paths or may be due to some other reason. Once again there is no explicit guarantee regarding the ordering of the packets. Obviously towards the end application this may not work at all in many cases. So in such cases where this is very important you have to take precaution against this or you have to put in some corrections for this at some other layer and the network layer is not doing this. This was the idea for breaking it up into layers in the first place.

In the physical layer it is the physical sending and in the data link layer sending is from one to one hop only and makes it as reliable as possible through checksum etc. In the

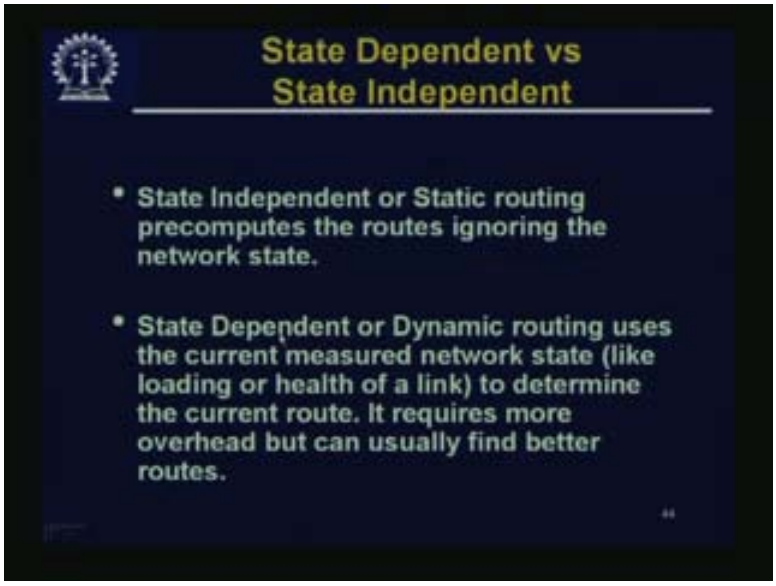
network layer it is just reaching the other end of the network layer through several hops. Now if you want to do it reliably you have to go up one level more and then try to do something there. We will see how it is done.

(Refer Slide Time: 52:48 - 53:16 min)



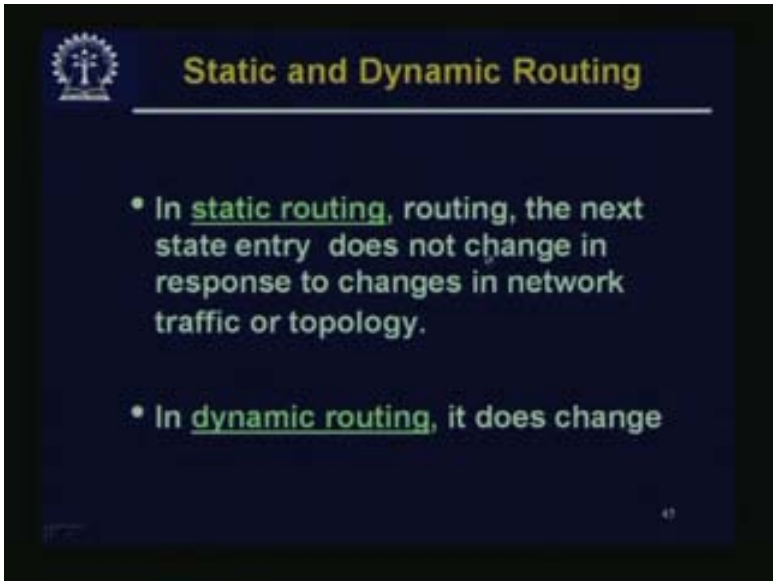
Single versus multiple paths: Each router maintains one primary and some alternate paths. Single path routing is used in internet to reduce routing table size. Multiple paths such as stochastic etc are not usually used in these routers in the internet because the routing table size is at a premium. Multiple paths are used by telephone networks as routes can easily be deciphered from the address such as telephone numbers.

(Refer Slide Time: 53:17 - 53:33 min)



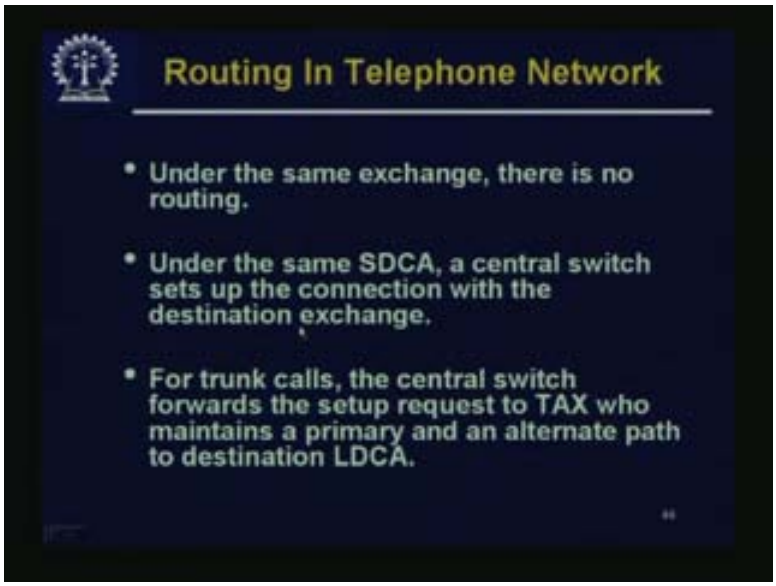
Next is state dependent versus state independent routing. State independent or static routing pre-computes the routes ignoring the network state and state dependent or dynamic routing uses the current measured network state (like loading or health of a link) to determine the current route which may change as the packet is proceeding. It requires more overhead but can usually find better routes.

(Refer Slide Time: 53:34 - 53:42 min)



In static routing, the next state entry does not change in response to changes in network traffic or topology. In dynamic routing it does change.

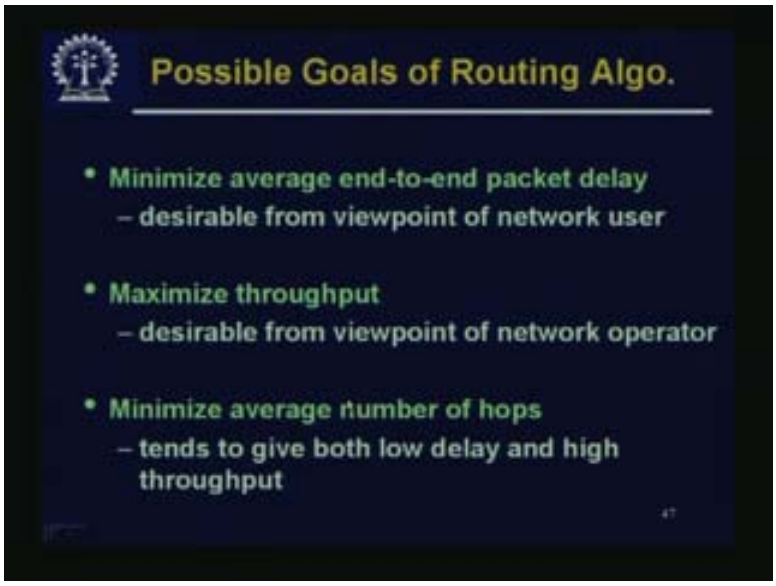
(Refer Slide Time: 53:43 - 54:08 min)



Routing in the telephone exchange of course is very simple as we have already seen. Under the same exchange there is no routing and under the same Short Distance Charging

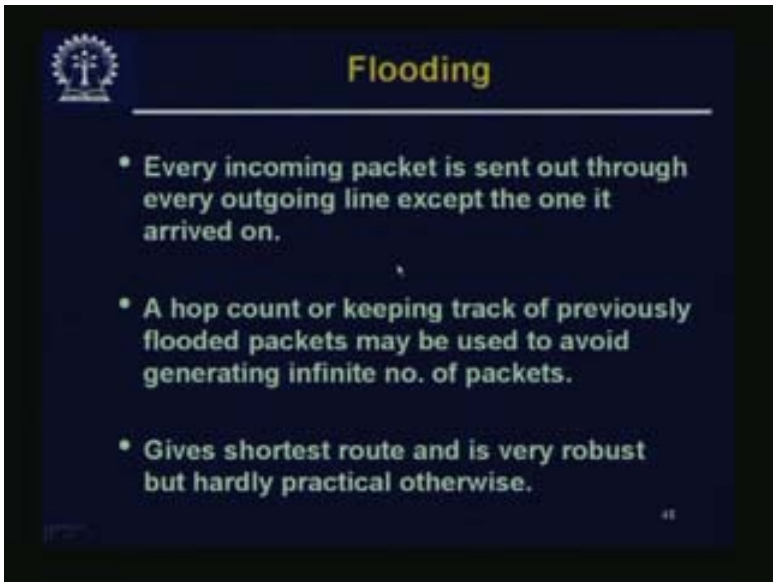
Area (SDCA) a central switch sets up the connection with the destination exchange. For trunk calls the central switch forwards the setup request to the trunk exchange (TAX) and maintains a primary and alternate path to a Long Distance Charging Area (LDCA).

(Refer Slide Time: 54:09 - 54:20 min)



The possible goals of routing algorithm may be to minimize average end-to-end packet delay (which is desirable from the viewpoint of network user), to maximize throughput (which is desirable from viewpoint of network operator) and to minimize average number of hops (which tends to give both low delay and high throughput.

(Refer Slide Time: 54:21 - 55:49 min)

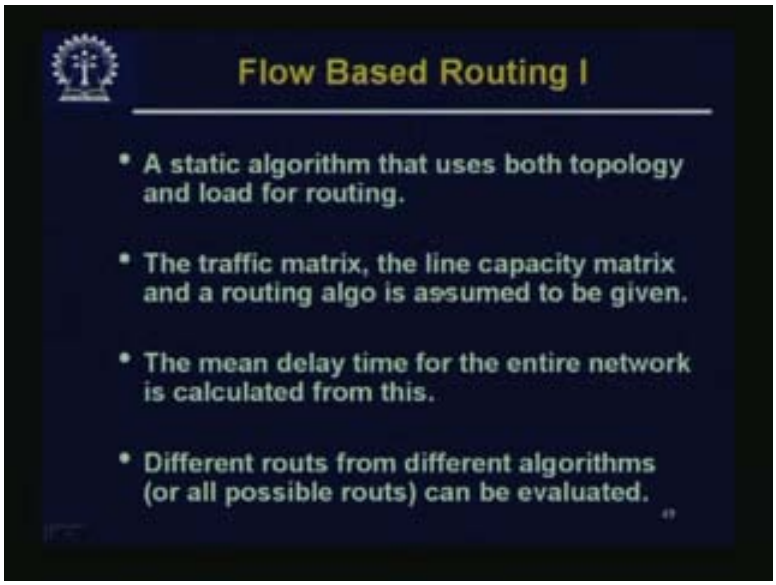


Another way we do routing route is by flooding. This is some kind of broadcast, so if a router wants to flood something it will send the same message to all the routers which are

connected. That may be a very nice and fast way of reaching somewhere because when you are flooding very soon this message will get replicated at each node and everything is running perfectly and in a synchronous manner it will reach the destination using the shortest possible route. The only problem is that not one copy will reach but multiple copies will reach using different paths. And then other copies will never get anywhere but they will sort of choke other parts of the networks so these overheads are there.

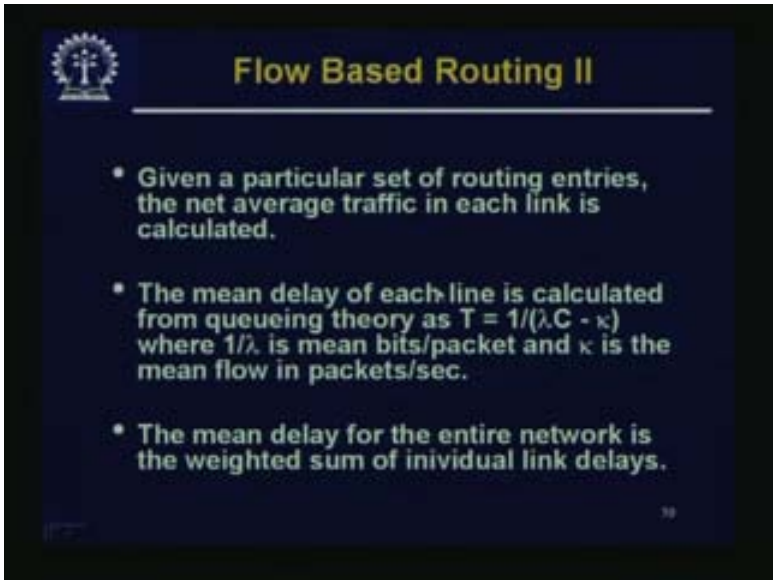
Still flooding is used in some special cases. This is one reason we use flooding and the other reason is that when we actually want to broadcast this to everybody then one good thing to do is to flood it. Every incoming packet is sent out through every outgoing line except the one it arrived on. A hop count or keeping track of previously flooded packets may be used to avoid generating infinite number of packets. Flooding gives the shortest route and is very robust but hardly practical otherwise. But in many situations they are also practical.

(Refer Slide Time: 55:50 - 56:06 min)



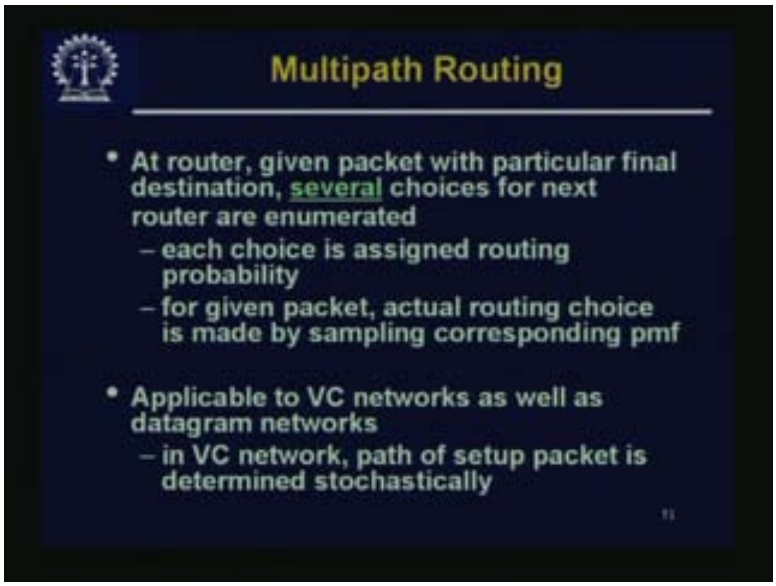
Flow based routing is a static algorithm that uses both topology and load for routing. The traffic matrix and the line capacity matrix and a routing algorithm is assumed to be given. The mean delay time for the entire network is calculated from this. Different routes from different algorithms (or all possible routes) can be evaluated.

(Refer Slide Time: 56:07 - 56:20 min)



We will come to that later on when we do MPLS. Given a particular set of routing entries, the net average traffic in each link is calculated. So you can try to do some traffic optimization through this.

(Refer Slide Time: 56:21 - 56:33 min)

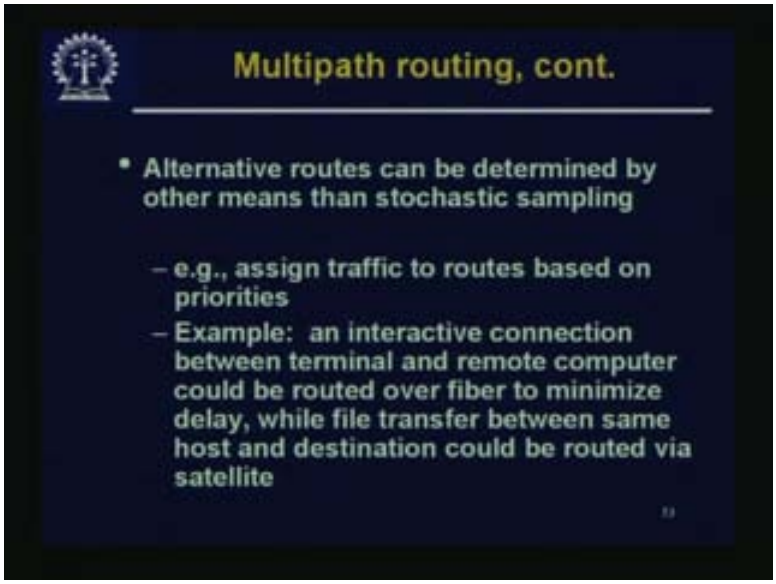


Then we have multi path routing. At the router, for a given packet with particular final destination several choices for next router are enumerated, and then the actual path is chosen in some fashion.

(Refer Slide Time: 56:34 - 56:42 min)

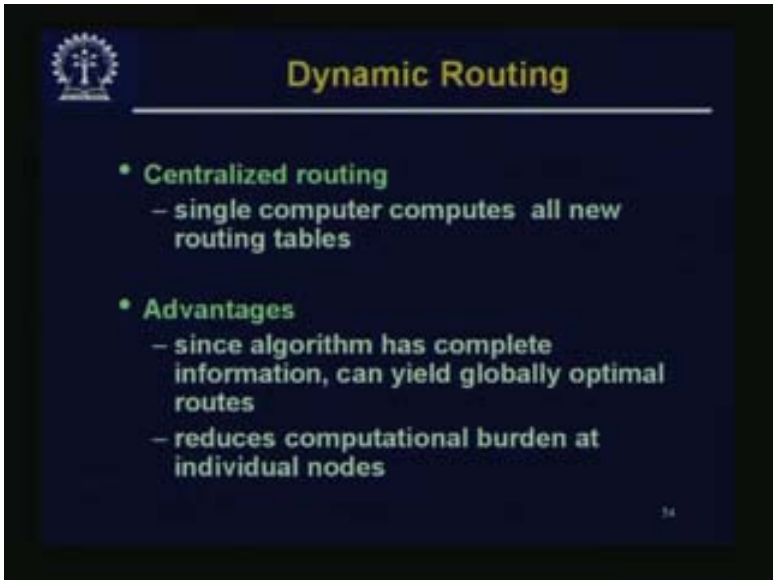
Multi path routing may yield more stable traffic.

(Refer Slide Time: 56:43 - 56:46 min)



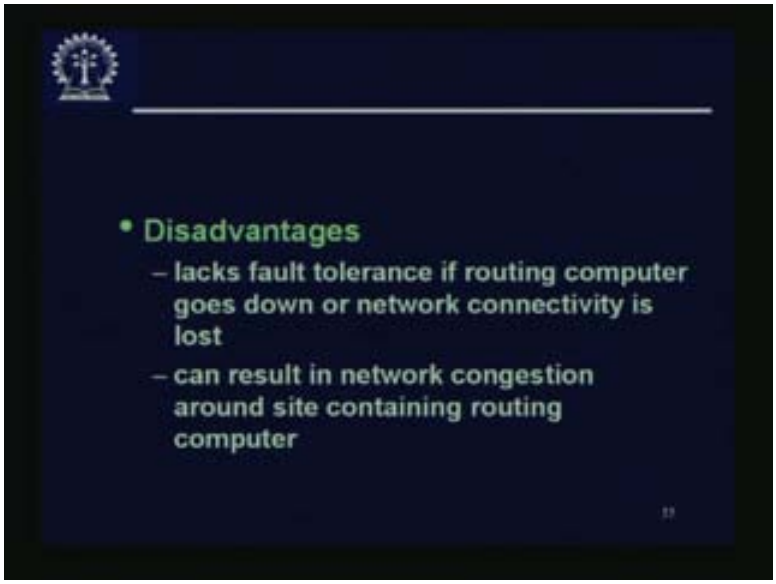
Alternative routes are also similarly determined.

(Refer Slide Time: 56:47 - 56:53 min)



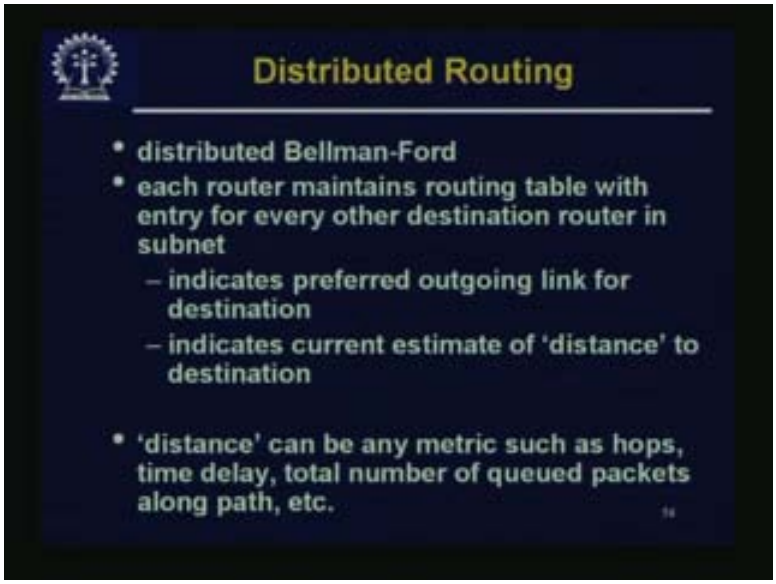
We have already talked about dynamic routing versus centralized routing.

(Refer Slide Time: 56:54 - 56:58 min)



It has its own disadvantages meaning it lacks some fault tolerance if routing computer goes down.

(Refer Slide Time: 56:59 - 57:23 min)



Distributed routing is the most usually used. It may use some distributed algorithm like distributed Bellman-Ford or it may use some centralized algorithm with distributed global data. We will look at distributed routing in more detail in the next couple of lectures.