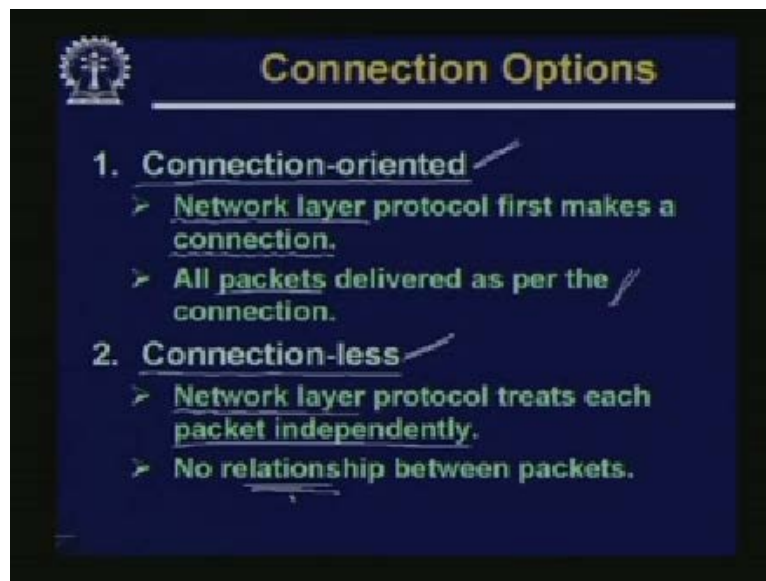


Internet Technology
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture No #07
Internet Routing Protocols Part-I

Today, we shall start our discussion on internet routing protocol. Now here we shall be talking about some of the ways in which the routing of the data packets actually takes place in the internet scenario. You may recall that in the last few classes we have already discussed a few things related to IP addressing and some routing characteristics of these IP addresses. In particular we had talked about the IP address masks we had talked about the classless internet domain routing and we had also talked about the variable length subnet masks. Now using these technologies we can make more efficient utilization of an available address block. Depending on the requirements of an organization we can suitably partition the addressees and make suitable subnets designed as per the needs. Now today we shall primarily start our discussion on the actual routing protocols which you people use in the internet scenario.

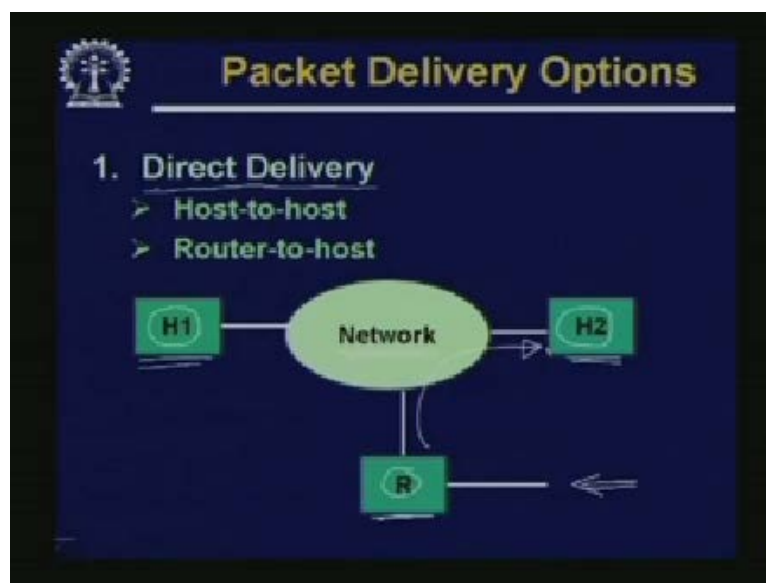
(Refer Slide Time: 02:02)



Now to start with the way you talk about some of the connection options. Now broadly speaking, when we talk about two computers on the internet trying to send and receive packets between themselves, we can either have connection-oriented approach or we can have connection-less approach. Now in the connection-oriented approach, this is essentially what we know as the virtual circuit mode of data transfer. Here basically the first step before any data transfer can take place is to have a connection established between the two parties. And the establishment of the connection is the responsibility of the network layer. And once the connection has been established all the packets would be delivered along the path that has been established as part of connection. And all the packets will be following the same path this is one characteristic of the connection-oriented approach. The other alternative is the connection-less approach where we do not explicitly establish any connection rather the network layer which exists in the different computers and intermediate nodes.

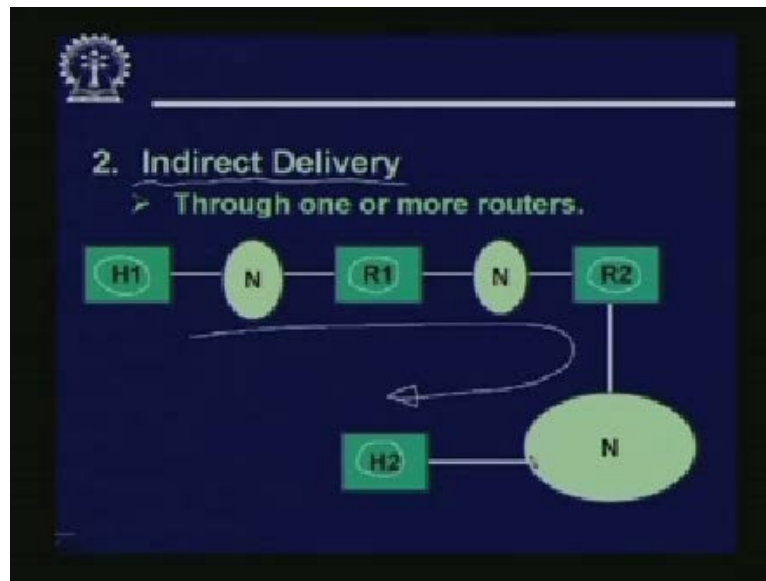
They treat each of the packets in an independently; which means that each of the packets are sent as an independent entity and no explicit relationship is maintained between the packets. This is the so called virtual, means a just as an opposed to the virtual circuit approach in connection-oriented. This connection-less means the datagram approach. Now in this datagram approach if you recall there was some problems that it face sometimes like the packets may be delivered out of order then the packet transit time may not be in determinate state. And in general it may be a little problem to support real time applications on this kind of technology. But the matter of fact is that the IP protocol on which actual the internet protocols are based today applications are based today. They in fact use the connection-less approach. So in the internet we are more uh you can say more familiar with the connection-less mode of data communication.

(Refer Slide Time: 04:46)



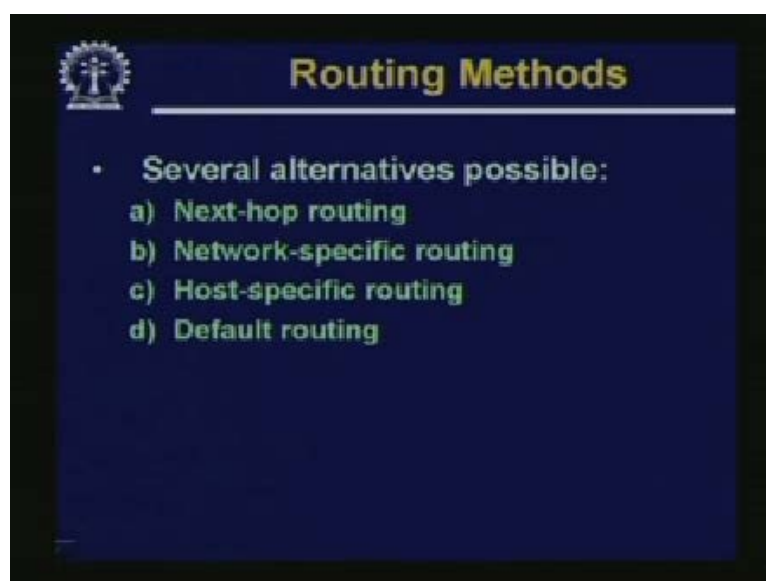
Now let us look at the various packet delivery options between two nodes in the network. The first approach is known as Direct Delivery approach. Direct Delivery means this can be either a Host-to-host. Suppose this is a network and we have one host H1 out here another host H2 out here and there is a router R. Direct delivery means packet gets transmitted from one node to the other without the packet being made to pass through any intermediate router. So in the Host-to-Host mode for example, this host H1 wants to transmit a packet to H2 both are connected to the same network. So the packet transfer can take place directly between them. Similarly you can have a Router-to-Host connection where possibly a packet is coming from the outside world and it reaches the Router the Router which is also connected to the network can directly send the packet to the host H2 say. These are examples of direct delivery of packets.

(Refer Slide Time: 06:04)



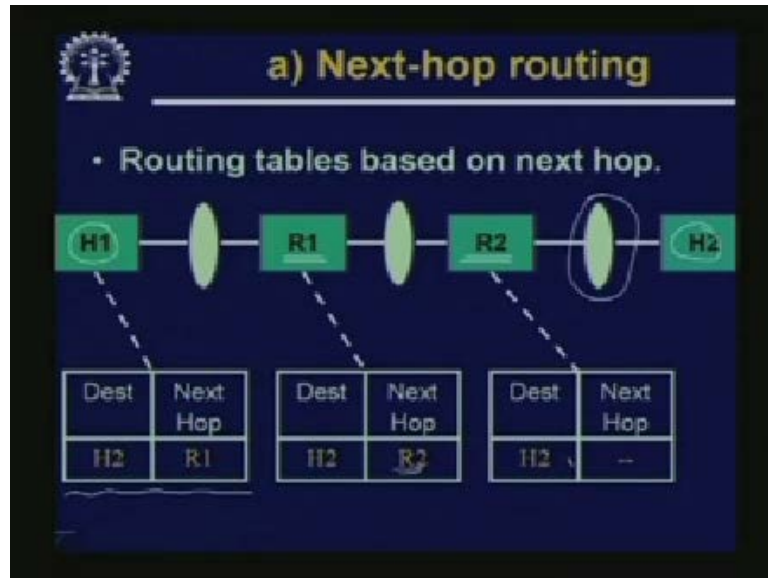
Similarly we can have Indirect Delivery. Now Indirect Delivery as opposed to the Direct Delivery approach here, whenever there two nodes one to send data from one to the other they will have to go or pass through one or more intermediate routing nodes. Let us see how this looks like. Just with respect to this diagram, suppose this host H1 wants to send a packet to this host H2 Now as you can see this path which needs to be followed and this path goes through two intermediate routers R1 and R2. So obviously in this approach these intermediate routers must take some routing decisions. Because these intermediate routers maybe having more than one possible outgoing link for an incoming packet. So the router will have to decide in order to send the packet finally to H2 which is the best outgoing link to select. So in this distributed way the decision is taken distributed on all the routers the packet will finally reach the final destination.

(Refer Slide Time: 07:29)



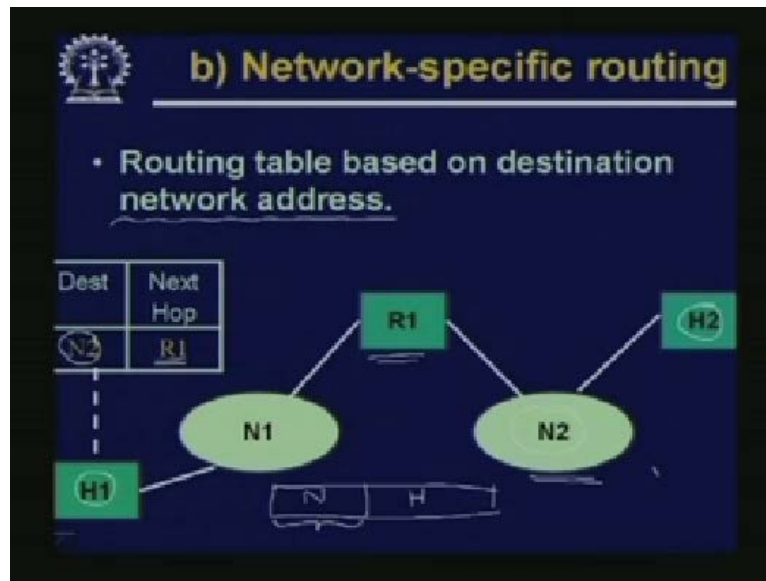
Now talking about the routing methods there are several alternatives possible. In fact there are 4 approaches. Next-hop, Network-specific, Host-specific, Default, there can be combinations of all these. So let us try to see how these alternate approaches are in fact these different approaches will actually control or will actually influence the way the routing tables are created and stored and processed in each of the intermediate routers.

(Refer Slide Time: 08:09)



So let us first see the Next-hop routing approach. Next-hop routing says suppose this is my source H1 and H1 sends a packet to the destination host H2. Now as this diagram shows that the packet has to flow through two intermediate routers R1 and R2. Now there are a number of hops this packet is having to take H1 to R1, R1 to R2 finally from R2 the packet gets delivered to H2. Now each of these routers as well as the host will be maintaining or will be having a routing table of its own. For example H1 will be having a table like this. This will say that if the destination of the packet is H2 then my next hop will be R1. Similarly for R1 there will one table entry which will be containing something like if the destination is H2. Then my next hop will be R2. Similarly for R2 it says that if it is H2 then already it is in the same network. Because both R2 and H2 are connected to this same network so there is no further routing required. So as you can see in this approach every router basically concerns itself with providing the next hop path for the packet given the destination address it will try to find out which is the next hop to be taken hop. Means it can be a router it can be the final destination host so it takes a decision in this regard. This is the next-hop routing approach.

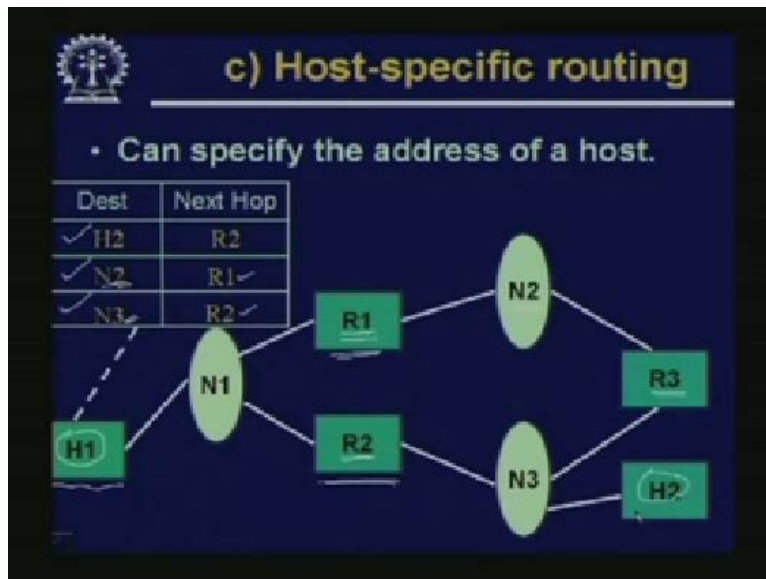
(Refer Slide Time: 10:00)



The next approach says that the table may not contain information about individual hosts rather it will be network specific. Here the routing table will be based on destination network address. Well here again let us take an example. This H1 is the source, H2 is the final destination. Now as you know that in the IP addressing, a typically IP address will consist of two parts. One will be the network part of the address; other will be the host part of the address. Now typically all the routers will only look at the network part of the address to take the routing decision. So basically this approach is based on this principle. Now as you can see at the routing table which is there for the host H1. It says that if the destination is the network N2, see here there is a difference as compared to the previous approach.

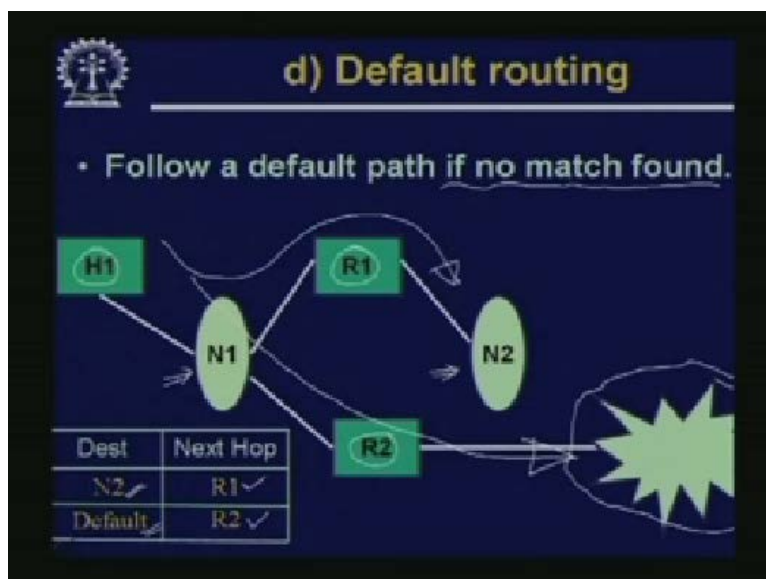
In the previous approach we are saying that in the routing table the destination will be referring to the IP address of a destination host. But actually if you look at the destination host IP address there will be a part of it which will contain the network address and there will be another part which will be containing the host address within that network. So if the packet can be made to reach the final destination address then also our purpose will serve. So in this method what we say is that if the destination network address is provided then the table will give you the next hop for that. For example from H1 if you want to go to N2 then this router R1 is the next hop you will have to first send the packet to R1 and R1 is already in this network N2. This router R1 and this host H2, both are part of this network N2. So no other routing is required. This is the second approach.

(Refer Slide Time: 12:24)



The third approach says this is you can say a combination of both this also allows host specific routing. Say you take this example here we have two hosts H1, H2, and there are several routers R1, R2 and R3 and you can say there are three networks N1, N2, N3. Now in the routing for host H1 there can be some entries for hosts. There can be some entries for networks. Like the first row of the table says that if the destination is the host H2 then packet to router R2. So in order to reach H2, R2 is the next destination, intermediate destination through which H2 can be reached. Similarly when you are saying you want to reach the network N2, then for reaching N2 we have to go through R1. So as you can see for N2, we have to go through R1. Similarly for network N3 we will again have to go through R2. So the destination maybe a host, the destination may be a network. Irrespective of that the routing table will contain information to take a decision that which is the next hop the packet has to be forwarded to.

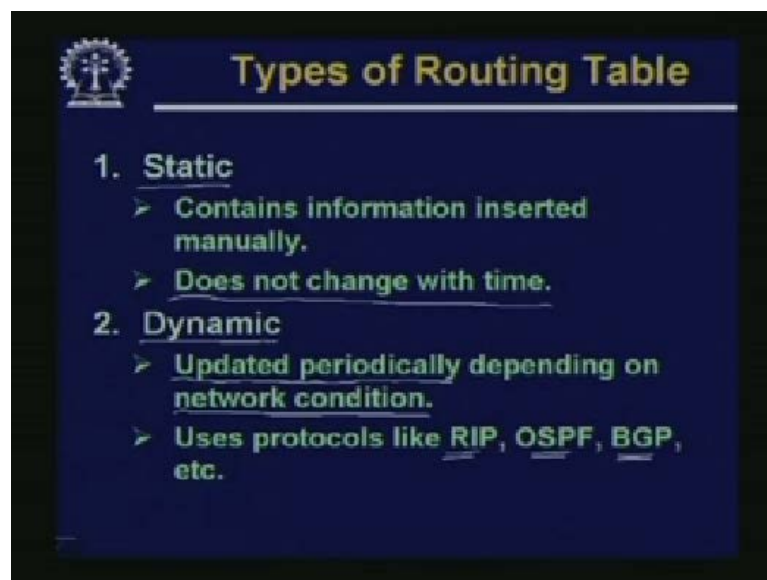
(Refer Slide Time: 14:08)



And any routing table will also have some mechanism for default routing. Default routing means what to do, if you do not find any match in the routing table corresponding to your destination. Now in reality you cannot expect that any address you give as the destination will have a matching entry in the routing table. Because there are millions and millions of computers all around the world there can be millions of possible addresses and obviously the size of the routing table will be limited. So the routing table will typically contain those entries which are most commonly used for the networks to reach your packets will most commonly flow. In addition it will also contain some default. If no match is found, where to send the packet next. So in this approach the default routing approach. So if you look at the picture the picture shows a host H1, two routers R1 and R2 and two networks N1 and N2.

Now in addition, you can also see there is an external network shown which is connected to R2. This external network can be the internet and whatever else we have shown in the diagram that may correspond to our internal organisation land. So we are now trying to find out a solution that from within our organisation land when we have to send to packet to the outside world and when not to. So again for the host H1 a typically routing table may look like this. Suppose if we want to send the packet to the network N2, then the preferred next hop is R1. For reaching N2 you have to go through R1 following this path. But if there is no match and the default in the routing table will take of those no match conditions. It says that if the destination address does not match any of the entries then you take R2, as the next hop as you can see; now the path followed will be like this. So from H1 to R2 to the outside world. This, the typical scenario.

(Refer Slide Time: 16:48)

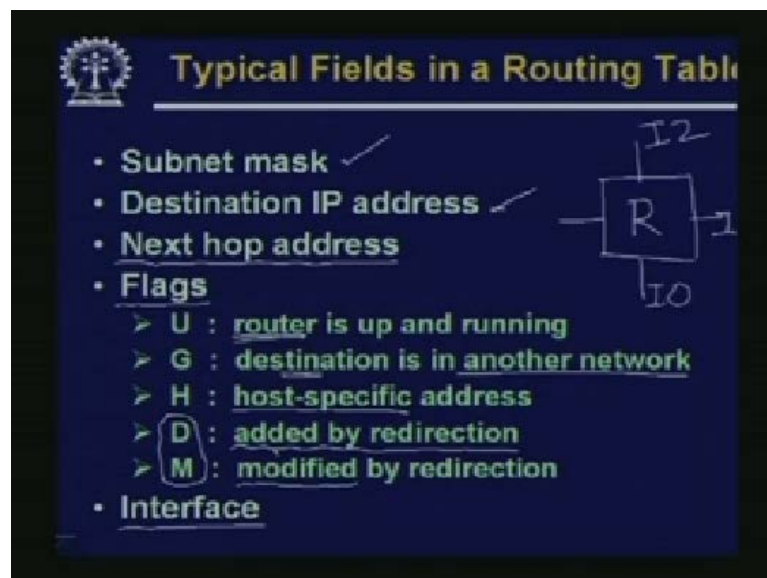


Now let us talk about the types of routing tables that you can have. Because an understanding of this will help us in understanding the requirements. That means what are the requirements practical routing protocol or algorithm should have in order this. The routing tables can be maintained in a proper way. Now broadly speaking routing tables can be either Static or Dynamic. Static as the name implies in a Static routing table the table is created once in the beginning and it does not change with time. Now Static routing tables are advantageous in

situations where there are very small changes in the network over a period of time. Most of the information in the network in terms of the nodes and the links they are fairly constant and if we can manually determine the best paths for every source destination pair, for example and if you can populate the routing table with those manually generated information, this will provide you the best possible routing.

But in practice the situation is not so simple. Our network is very large we are a part of the internet and here we can see some computers can enter a network. It can come out, it can go down, some link may fail, some router may fail, some may new router may get added. So there are a lot of changes that can possibly take over a period of time. In the Dynamic routing table these kinds of changes can be incorporated. So as the name implies Dynamic means that these routing tables are updated periodically and this updation obviously will be done depending on the condition of the network. And practical protocols like RIP, OSPF and BGP we shall be looking briefly into this protocol very shortly. These protocols in fact are all Dynamic protocols in the sense that they can Dynamically update the routing tables in response to change in the network conditions.

(Refer Slide Time: 19:20)



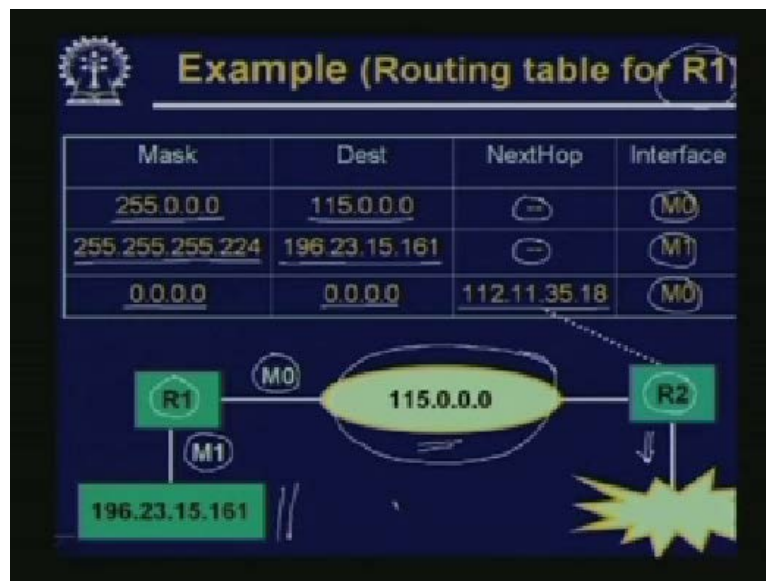
Now let us talk about the typically fields in the routing table of a practical system. Well, in the examples that I have shown earlier we had taken a very simple example and try to illustrate with that. But let us take a real router or a real host where there is a routing table. So exactly what are the information we need to keep in the routing table? Let us see some of the typical fields. Well a routing table will clearly contain the destination IP address and the subnet mask. These two are absolutely essential. Destination IP address along with subnet mask will give you the information regarding which address class it belongs to whether you are using subnetting or not. And if there is a match you will obviously also have to specify the next hop address. Meaning, if your destination address matches this entry of the routing table then what should be the next hop? Where you should forward the packet?

In addition the routing table will contain several flags which will tell you something about the particular row of the routing table. For instance if the flag contains the symbol U, this means

that the next hop router which this routing table entry refers to, is presently up and running. Which means that the routing table of the particular node which we are considering that particular node knows that particular router is up and running at this present point in time if the flag is G. This says that your destination is not in the same network it is in another network. If it H this means that whatever address is specified in the routing table that refers to the address of a host and not a network. So if this H is not present it will automatically imply that it is a network specific address and these flags D and M indicate that some dynamic updation has been carried out. Depending on the information you have received from the neighbouring nodes there is something called redirection.

If some of the neighbouring routers find out that a better path to a particular destination is available, then that information will immediately be informed back to the router under consideration. This router under consideration will be making appropriate changes in the routing table and will be setting the flag to D. If this is a new entry which is being added or M if an entry which was already there is getting modified. Well in addition to all these three routing table will also contains interface information. What this means is that if you consider a router as a box like this suppose this is your router. This router can contain several interface quotes. This interfaces means you can have names I 0, I1, (23:08) I2, etcetera. So whenever you have an entry specifying the next hop address, whatever you will also have to specify that through which interface port of the router this information has to go out.

(Refer Slide Time: 23:27)

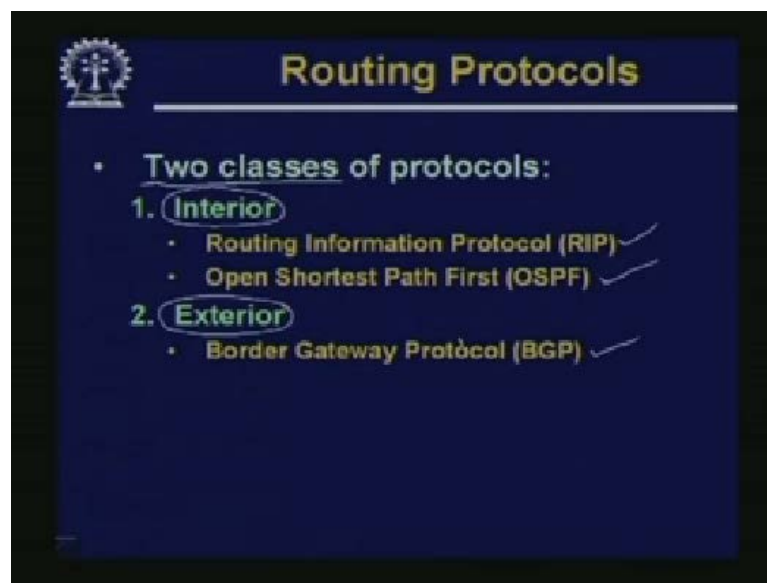


So this slide shows a small example to illustrate the routing table, including some of these features of course here we are not showing the flags. Here we are considering the routing table for the router R1. This is your R1. The first entry says that your destination is 115.0.0.0 with a mask of 255.0.0.0. This clearly means that this is a network address and your next hop does not contain anything which means that this refers to the same network in which the router is connected to. So the router is already connected to the same network, so it does not have to send it to anywhere else. The only thing to specify is that the packet has to come of interface M0 of the router; the router has two interfaces M0 and M1. The second entry says that the destination is 196.23.15.161. This is the address of a host. This is an example of a

host specific entry in the routing table. Here the mask specifies the corresponding network mask it specifies also that it is a class C address which is getting subnetted. Next host empty again means this also refers to the same network and the interface M1 says that this has to go out through the interface M1.

The third interface you can see it refers to an address where destination as well as mask are all zeros. Now as a matter of convention the all zero address is the default route or default address is represented by the all zero factors. So this last entry refers to the default case. But the next hop is specified as some address which is address of some other router and in order to send there you have to again go out through interface M0. Because through interface M0 you reach this particular network and this router R2 is also connected to this network. So this packet will be reaching R2 and the R2 can help in sending this packet to the outside world. This is how the routing of the packets take place in a practical scenario. Now we shall look at some of the practical routing protocols which are actually implemented in routers and the other systems which you see around us. This will give us some idea about the complexity of the problem in one and on the other hand. We shall also try to apprehend the kind of requirements or the kind of algorithms that the router has to run in order to have these implementations in place. So the first set of routing protocols are RIP and OSPF.

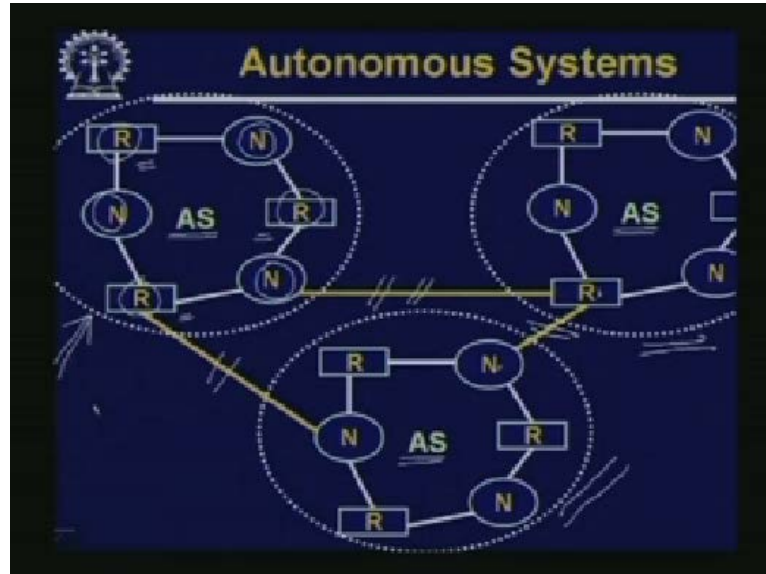
(Refer Slide Time: 26:51)



But before going in to that, let us first talk about a broad classification of routing protocols. Broadly, routing protocols can be categorized as either Interior or Exterior. Now interior exterior, the distinction we shall be talking about very shortly. But to talk in a very simple term, interior routing protocol means the protocols that all the routers which are inside my organisation, they use to keep their routing tables updated. So the interior routing protocols are specific to my own organisation. My organisation maybe having 10 routers inside and they keep each other informed and keep routing tables updated by exchanging some sort of information. This is the purpose of the interior routing protocols and 2 representative protocols in this category are RIP and OSPF. Routing Information Protocol is the older of these two and OSPF or Open Shortest Path First is the more popularly used today. An exterior routing protocol in contrast refers to the protocol which routers use which are across

networks across organisations. They are connected possibly through wide area network links. They use some protocol to keep their tables updated. So this is the exterior routing protocol and the most common protocol used here is called BGP or Border Gateway Protocol.

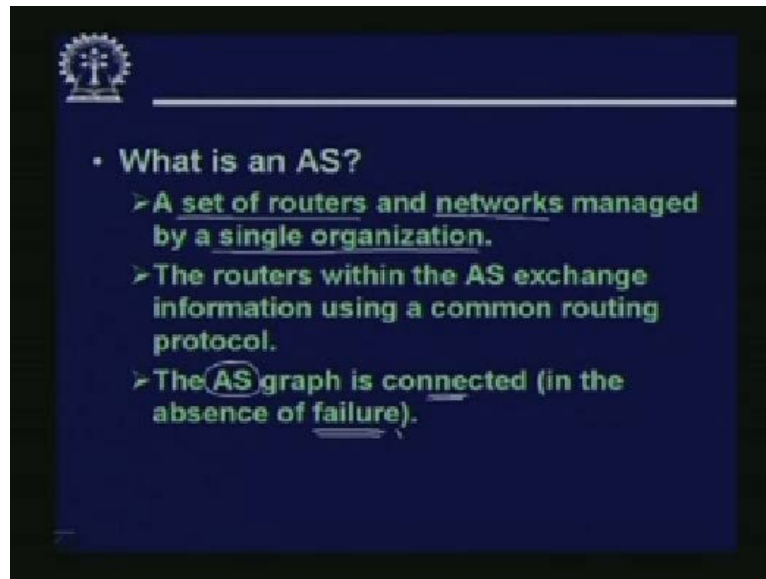
(Refer Slide Time: 28:40)



Let us first look into the concept of an autonomous system which is central in understanding any one of these three protocols we have just mentioned. The concept of autonomous system is essential in having any one of these three routing protocols in place. So let us try to understand what is meant by an autonomous system. Now in this diagram these three dotted regions that we see they refer to autonomous systems in short AS. So this diagram shows three autonomous systems. Now from the practical point of view an autonomous system may refer to a particular organization. A particular organization as I had said may be having several routers, several networks and they are all connected among themselves. Like for example say in an education institution you may be having several departments. They may be having their own networks and these networks maybe connected through routers. So this is how an autonomous system may be built. So as you can see that this autonomous systems which I have shown in this diagram they consists of some routers.

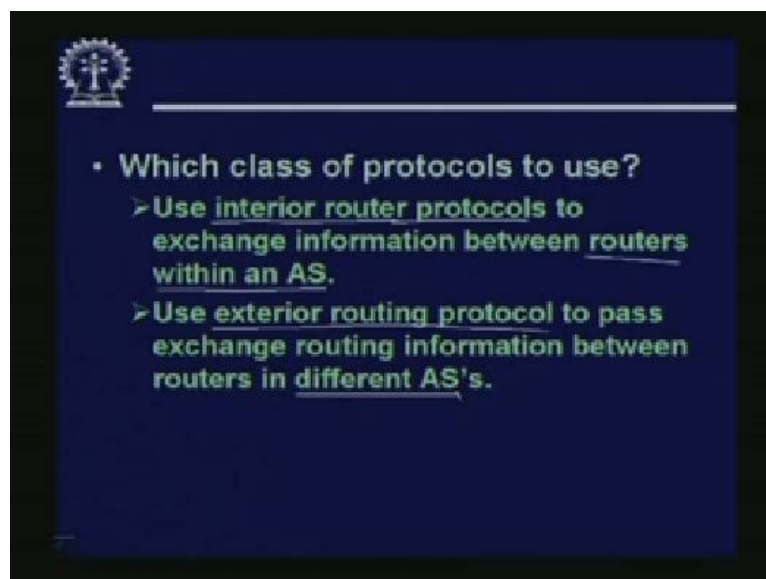
They consist of some networks and across autonomous systems there are some connections, some router maybe connected to some other networks. Some router may be connected to some other network. This router may be connected to this network and so on. So in this diagram there is a cyclic path, but in general such cyclic path may not be present. But this diagram gives you, shows you the problem in the overall perspective within these dotted regions which are the autonomous systems. There are several routers and whatever way these routers exchange information among themselves. To keep them updated these are under the jurisdiction of the interior protocols routing protocols. But across the networks, for example something might have gone wrong in this first autonomous system. Maybe some link is down or some network is unreachable. But the routers the other autonomous systems they may not be knowing this. So through the exterior protocol (31:20) through these thick links. Some information will be exchanged across the autonomous systems through which the routers can also get their tables updated.

(Refer Slide Time: 31:40)



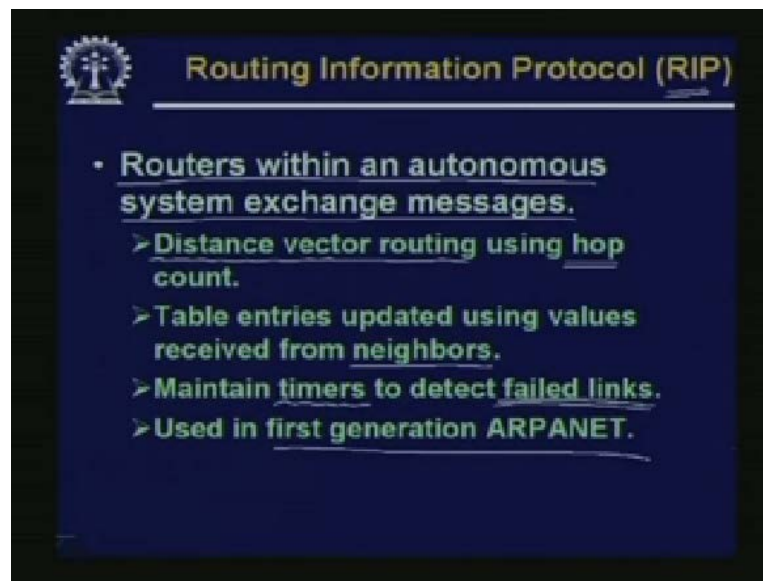
So to define an autonomous system you can define an autonomous system quite loosely as a set of routers and networks which are typically managed by a single organization. They are part of a single organization an autonomous system refers to the network of a single organization and it can be a collection of several networks and routers. So the routers within the AS will exchange the information using the common routing protocol which is an interior routing protocol as I had mentioned. And the graph interconnecting the autonomous system must be connected because if they are not connected then obviously some of nodes are not reachable from somewhere else. So unless there is a failure there is an explicit link disconnection the AS graph, that means a graph at the AS or the nodes and interconnection at the edges the graph will remain connected. So the graph may become disconnected when there are failures. But otherwise they will have to be connected.

(Refer Slide Time: 32:50)



Now as I had just mentioned that which class of protocols to use where? You will be using interior router protocols for updating routers within an autonomous system? In contrast would be using the external or exterior routing protocols for routers belonging to different autonomous systems. So in this way all the routers can be updated, they can keep their routing tables up to date by exchanging information. This is some kind of a hierarchy you can see at the highest level you have the BGP protocol running which is more like a global message exchange in the local context within an autonomous system. It is the interior protocols which are running to keep the routers inside an AS updated.

(Refer Slide Time: 33:52)



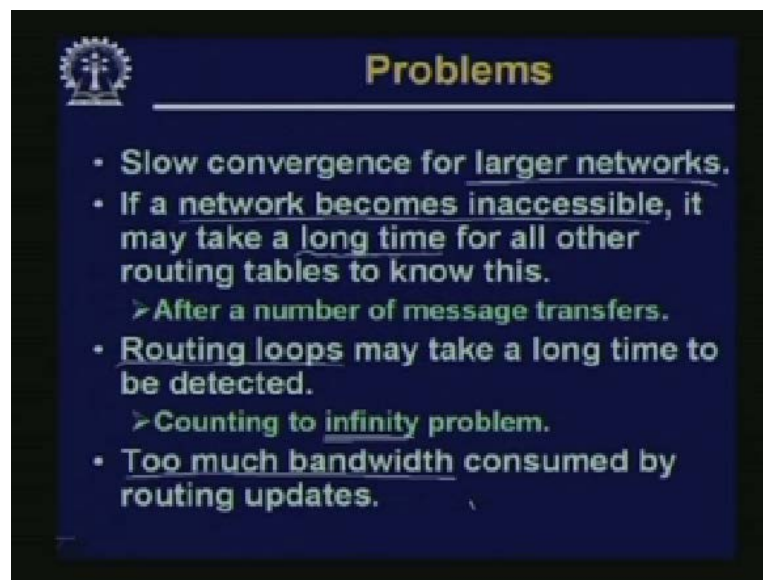
Now we start with a brief introduction to the Routing Information Protocol in short RIP, which is an interior routing protocol. So as I had mentioned using RIP, routers within an autonomous system can exchange messages. Now I repeat the purpose of this message exchange is to update their routing table with the latest information about the network. Some link may become congested, some link which was previously congested. Now it is very smooth, some link may have gone down, some link which was down may have gone up, some many different kinds of dynamic events may occur. So this RIP protocol in order to keep the tables updated they use the well-known distance vector routing and distance is calculated in terms of the number of hops. Now if you recall distance vector routing basically is a method where each of the routers will contain information about all other nodes and how far they are.

And distance is estimated in terms of the number of hops, if there are two routers I have to go through the number of hops will be three. So here periodically each of the neighbouring routers suppose I am a router I have 4 routers in my neighbourhood. So all my 4 neighbours will be sending me information about their connectivity with their neighbours. They will tell me that are far are the other routers are from them maybe they some updated information as compared to myself. So I can find out for example for a router x my table shows that the distance from me to x is 5 hops. But one of my neighbour says from that neighbour says the distance of that router x is only 3. So 3 plus 1, there is a new link I have found out which can

reached in 4 hops. So I immediately update my routing table with that information that in order to reach that router x.

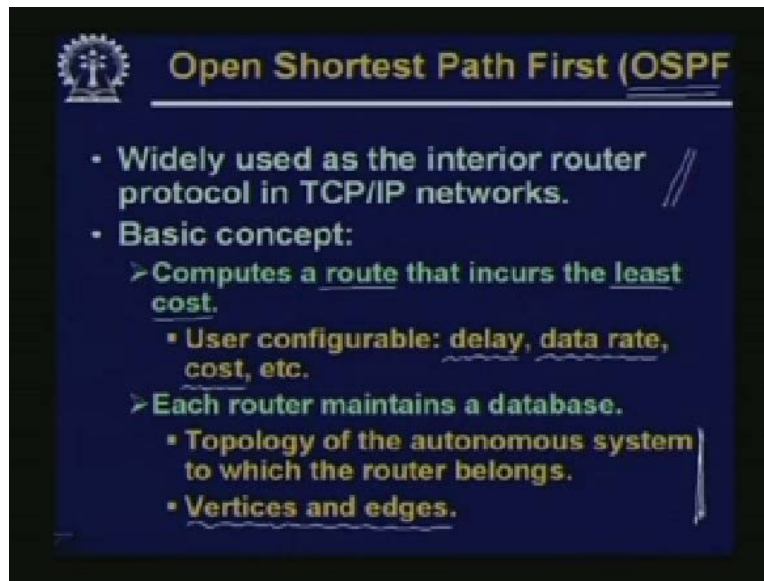
Now let me go through my new neighbour who has informed me with this new path, new route. So in this way all the routers exchange periodic message only through their neighbours not everybody and through these neighbour information these tables get updated continuously. So as I had mentioned the table entries get updated by values which are received only from the neighbours and in order to detect failed links the routers maintain timers. How suppose I have a neighbour say y, who is supposed to send me periodic updates? But I have found out even over a period of time I have not received any. Any information from that so if my timer expires then I will declare that the particular link is down. So I can update my table accordingly and send the information to other neighbours also. This approach was used in the first generation of ARPANET. But as mentioned this is an old protocol.

(Refer Slide Time: 37:34)



There are a number of problems. For large networks the convergence is slow that means the updation that takes place very slowly across the network. And if due to some link failure some network or a part of the network becomes inaccessible. Then it may take a long time for the others to know about this event. That means it can take considerable amount of time for the routing tables of the other nodes. In the other part of the network to get updated in a suitable way to reflect this change. This may require number of message transfers and there is also the possibilities of routing loops. Because since the tables are not updated simultaneously there can be some inconsistencies at some point in time. So a packet may be moving along in a cyclic path across some nodes in the graph. There should be a way to stop these stop these packets from going around the cyclic path indefinitely some hop count or something can be maintained. This basically a counting to infinity problems something like this. But in fact instead of infinity the packet header is loaded with some number which is decremented at each hop and whenever it reaches zero the packet gets discarded. Now to summarize this protocol consumes too much bandwidth just for updating the routing tables.

(Refer Slide Time: 39:08)

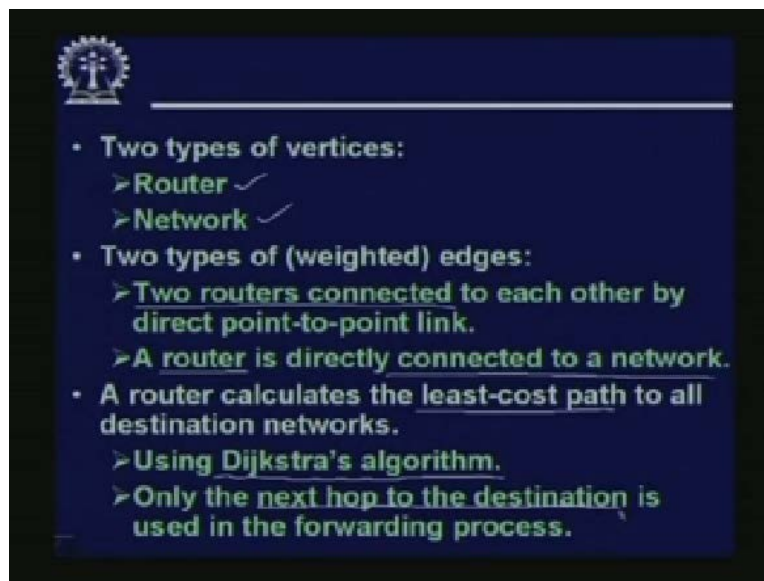


Open Shortest Path First (OSPF)

- Widely used as the interior router protocol in TCP/IP networks.
- Basic concept:
 - Computes a route that incurs the least cost.
 - User configurable: delay, data rate, cost, etc.
 - Each router maintains a database.
 - Topology of the autonomous system to which the router belongs.
 - Vertices and edges.

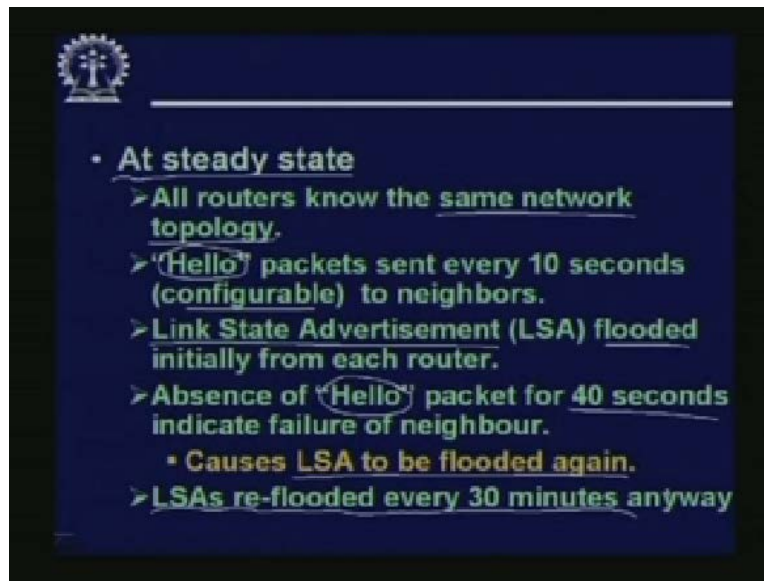
So what people have done, they have come up with a protocol OSPF which is widely used today as the interior protocol in TCP IP networks? The basic idea is similar to the IP. Here you try to compute a route that incurs the least cost. Now the notion of the cost is not fixed here. This can be configured by the user. The user depending on the requirement he can specify the delay as the criteria data rate as the criteria the actual monetary cost or the rental as the criteria and so on. So you can compute a route that will incur the least cost and each router will maintain a database and these databases will contain the entire information of the autonomous system. Now in general this is possible because an autonomous system is under the jurisdiction of a single organization. So the network manager of that organization can load the routing tables of all the routers with the complete information. This database can exist in all the routers. Database basically consists of the topology of the autonomous system. The vertices which are the networks and routers and how they are interconnected. This database is maintained by each of the routers.

(Refer Slide Time: 40:43)



And in the graph as I had mentioned there are two types of vertices in the graph; router graph and network graph. And the edges may represent two routers which are connected to each other or a router which is connected to a network there are two kinds of edges. Now in OSPF since everything belongs to the same network and mostly the information available in all the routers are accurate because it is under the same network same organization. So you can apply some least cost path like the Dijkstra's algorithm for calculating the best path to all destination networks. So essentially every router computes the best path to all the other networks. This is the approach followed and the well-known Dijkstra's algorithm is used in OSPF for this purpose. And when the routing tables are populated again only the next hop to the destination is stored there because the entire shortest path need not be stored. Because anyway all the routers are calculating it anyway suppose I want to send it to a final destination x I just find out that in the best path to x which is my next hop. So I simply follow the packet to the next hop. The next hop will again take the decision that for that particular next hop router to send it to x which is the best path. So in that way hop by hop the packet will move towards the final destination along the best path. This is the essence.

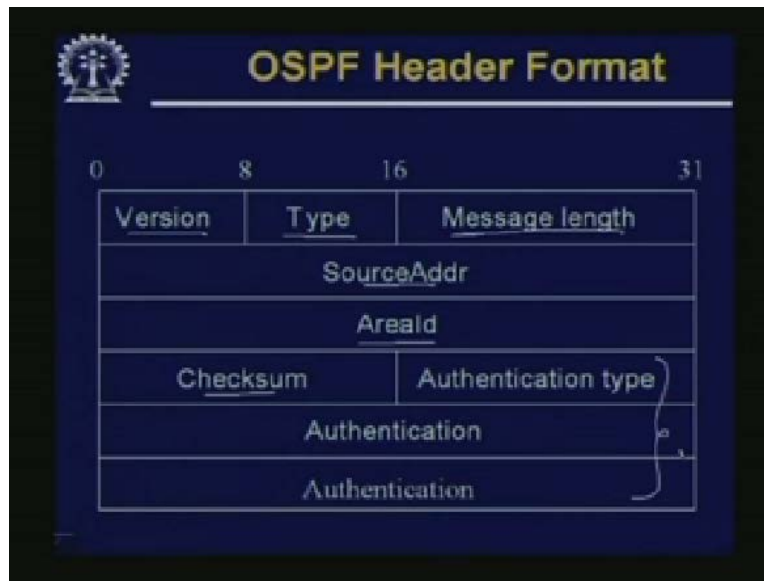
(Refer Slide Time: 42:31)



Now if there are no changes in the network very quickly then in the steady state all routers will have the same topology information with it. Now the way this OSPF works is that so called Hello packets are sent every 10 seconds are. So this time can be varied this is configurable to the neighbours. So every neighbour tells each of its neighbours that well I am alive I am not down I am up. So every 10 seconds or so this kind of Hello packets are sent to all the neighbours this keep the link up and running and Link State Advertisement packets are also sent from each router. This is like the distance vector routing approach. So I send my routing table to all other routers. Now unlike RIP I am not sending it only to my neighbours I am flooding it everywhere see everywhere it is possible to do here.

Because I am only talking about one autonomous system within a network so it is manageable. This is flooded k and if the Hello packet does not reach, if this Hello packet does not reach a particular node for more than 40 seconds, this will indicate the failure of that node or the link connecting that. So if this kind of a failure is detected again the Link State Advertisement of the updated routing table will be flooded again. So any router who as soon as comes to know about any change in the network immediately floods the LSA packet to everybody else so that everybody can keep the tables updated and this even if this kind of events do not occur. This LSAs are regular expression-flooded every 30 minutes in any case.

(Refer Slide Time: 44:34)



Now in OSPF there are a number of fields in the header. I am not going into details of this. Version of the OSPF which Type of OSPF packet you are sending, Message length, Source address. This is the AreaId which is the autonomous system id basically, Checksum and some Authentication related fields.

(Refer Slide Time: 44:56)

-
- Packet types :
 - >1 : Hello (check if neighbor is up)
 - >2 : Database Description (synchronize database at beginning)
 - >3 : Link State Request (request specific LSA)
 - >4 : Link State Update (LSAs flooded)
 - >5 : Link State Acknowledgement (flooded LSAs are explicitly ack'ed – reliable flooding)

Now, the types of the packets can be several one I have already mentioned the Hello packets. The Hello packets are used to check if the neighbours are up. Database Description packet, this is sent only at the beginning to load the routers with the initial tables. This is done by the system administrator at the very beginning by flooding a Database Description packet to all the routers. So the routers get their database updated using this. Then you have the Link State Request packet, this is a request. Specific LSA that means this is a Link State Advertisement.

Based on some specific request you have obtained from some host or somebody else who wants to make some changes in the table.

And this change has to be flooded immediately. Similarly the so called Link State Update, this if some link goes down there are some change in the network configuration. Again the LSAs will be flooded and Link State Acknowledgement packet is also used. For example even during flooding, whenever I flood a Link State Advertisement to everybody else. So whenever this flooding reaches I can say some other node that some other node will be sending an explicit acknowledgement back to me so I know that my advertisement or my broadcast was received correctly by that particular node. So this is because of this acknowledgement. This is also sometimes called reliable flooding with acknowledgement.

(Refer Slide Time: 46:50)

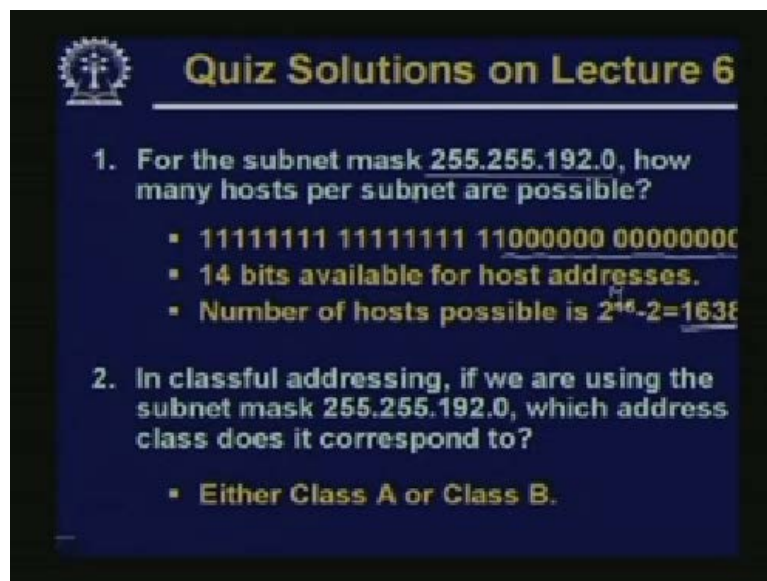


And Authentication I am not going into details of this. Because this OSPF depending on the environment where you are using, depending on the kind of network the kind of security you want to have in a network. You may want that whatever flows in the network should be encrypted in a proper way. There should be proper authentication. So there are ways of doing that well you may choose not to have any authentication. So everything will be going in Cleartext or you can have. Encryption along with authentication using MD5 or any other user defined algorithm is also possible. For example in my organization network I may choose to use my own pictographic schemes, my own encryption decryption schemes for securing my system. So with this we basically come to the end of this lecture. Now just to quickly summarize in this lecture we quickly looked at the different approaches to routing virtual circuit datagram was one thing. And again depending on whether we are trying to keep information about the final destination or the final network or default. So how the routing table will look like, what are the kinds of entries that a typically routing table can have these some issues related to these we had looked at.

Now in addition we have looked at a couple of interior routing protocols namely RIP and OSPF which are used by the routers that are inside an autonomous system. We had just mentioned that all the routers that are inside an autonomous system. They can use this RIP or

OSPF kind of protocol to keep their own internal tables updated. Now we have also mentioned that in addition to the interior protocols there are another class of protocols called exterior routing protocols which are used by routers across autonomous systems to exchange messages, to keep their tables updated. Well we shall be discussing this exterior routing protocol in our next lecture. But let me tell you one thing particularly the internet service providers the ISPs, the routers which they have they must be running BGP kind of exterior routing protocols because they need to keep their routers updated with respect to external routers their connectivity, their failure modes and so on. Now let us look at the solutions to the questions we had posed with regards to our previous lecture. Let us quickly go through them.

(Refer Slide Time: 50:18)



The first question was for the subnet mask 255.255.192.0, how many hosts per subnet are possible? Well this is fairly simple if you simply write down this address in binary you see that you have 14 0s at the end. So 14 bits are available for host address. So number of hosts possible is here this is a typo this should be 14, 2 to the power of 14 minus 2 which comes to 1638, 4 minus 2382. So its approximately 16000 hosts are available in this particular. Now the question was in classful addressing if we are using the subnet mask 255.255.192.0, which address class does it correspond to? See this cannot be class C because 192 means there are some bits in the third octet which are also zero. Now in class C we must have a subnet at least 255.255.255.0. But since this is less than 255, so it cannot be class C. But it can be either Class B or Class A because if we have Class exclamation or Class B you can have any number of the leading bits set to one in the subnet mask in order to have subnetting. So as a result just by looking at the subnetting you cannot distinguish whether it is Class A or Class B. It can be any one of them, but it cannot definitely be class C because class C must have all those bits in the third octet also one which is not in this case.

(Refer Slide Time: 52:11)

Quiz Solutions on Lecture 6

3. What is the subnet address if the destination IP address is 144.16.34.124 and the subnet mask is 255.255.240.0 ?

34 :: 0010 0010
240:: 1111 0000
AND:: 0010 0000

Subnet address will be
144.16.32.0

Third question. What is the subnet address if the destination IP address is this and the subnet mask is this? This is fairly easy. See, 34 and 240, you look at this. This is the part of the network because subnet mask says 240 is the subnet part. So you take these two parts, write down in binary, do a bit by bit ANDING, you get this 32. So your subnet mask or the subnet address will be 16.32.0. This is how we compute the address of the subnet.

(Refer Slide Time: 52:50)

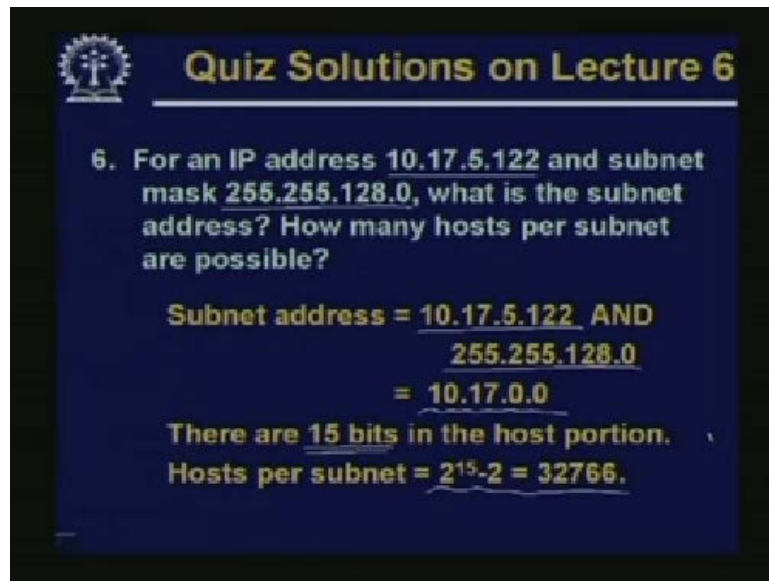
Quiz Solutions on Lecture 6

4. What is the natural mask for a class C network?
255.255.255.0

5. Using simple subnets, is it possible to divide a network into unequal sized subnets?
No. Simple subnets can only divide a network into equal-sized subnets.

Natural mask for class C network this is simple. ((52:58) Unable to hear properly) zero. Next question, using simple subnets is it possible to divide a network into unequal sized subnets? See if you have simple subnets. Then one basic thing is that all subnets must be of equal size. Because you are fixing up the number of bits that we are using to address. the hosts inside a subnet so all the subnets must be of the same size. So the answer is No.

(Refer Slide Time: 53:37)



The slide features a dark blue background with a white gear icon in the top left corner. The title "Quiz Solutions on Lecture 6" is written in yellow at the top. The main text is in white and yellow, providing a solution to a networking problem.

6. For an IP address 10.17.5.122 and subnet mask 255.255.128.0, what is the subnet address? How many hosts per subnet are possible?

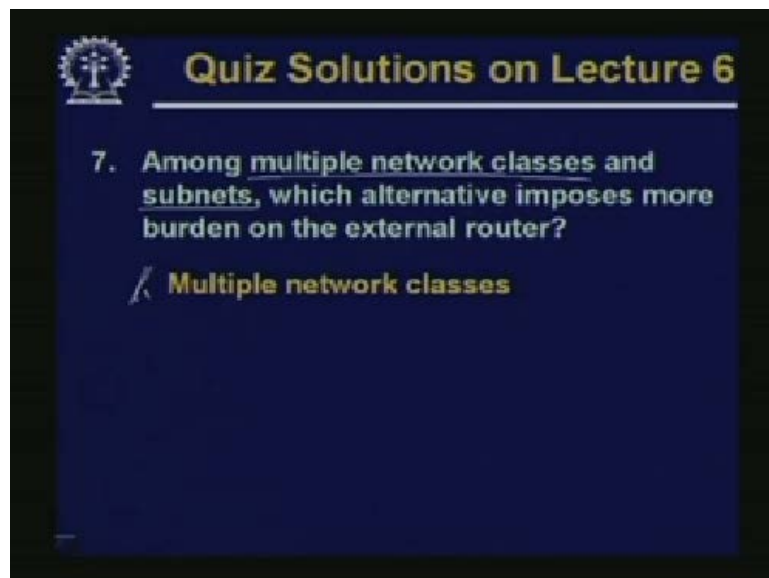
**Subnet address = 10.17.5.122 AND
255.255.128.0
= 10.17.0.0**

There are 15 bits in the host portion.

Hosts per subnet = $2^{15}-2 = 32766$.

6. For an IP address this and a subnet mask this, what is the subnet address? Subnet address again you can find out by doing a bit by bit ANDING. So the subnet address comes to 10.17.0.0. How many hosts? Well if you look at the subnet mask 2518 128.0, you will find that there will be 15 bits in the host position. There will be the 8 bits in the last octets, 7 bits in the previous octet. So the total number of hosts will be 2 to the power 15 minus 2 or 32766.

(Refer Slide Time: 54:06)



The slide features a dark blue background with a white gear icon in the top left corner. The title "Quiz Solutions on Lecture 6" is written in yellow at the top. The main text is in white and yellow, providing a solution to a networking problem.

7. Among multiple network classes and subnets, which alternative imposes more burden on the external router?

Multiple network classes

Well Among multiple network classes and subnets which alternative imposes more burdens on the external router? See multiple network classes you use multiple class C addresses. So number of entries in the routing table will be increasing. But in subnets the external routers will be having only one entry for the entire network.

(Refer Slide Time: 54:32)

Quiz Solutions on Lecture 6

8. Using VLSM, give a scheme to split a class C address into four subnets where the number of hosts required are:
100, 55, 20, 30

The diagram shows a binary tree starting with 256. It splits into two 128s. The left 128 splits into 64 and 64. The right 128 splits into 64 and 64. The left 64 splits into 32 and 32. The right 64 splits into 32 and 32. The final subnets are 100, 55, 20, and 30.

So the first choice will be imposing more burdens in terms of the size of the routing table. Well Using VLSM, we want to divide a class C address into 4 subnets of size 100, 55, 20, 30. It is easy in class C, the available size of 256 can be first divided into 128 and 128. This 128 can be divided into 64 and 64. 64 can be divided into 32 and 32. So this 100 you can assign to this 55 you can assign. Here 20 you can assign here and the last 30 you can assign here.

(Refer Slide Time: 55:08)

Quiz Solutions on Lecture 6

9. If the number of hosts required are 100, 50, 50 and 20, can VLSM be used?
X Not possible. The last subdivision of 50 and 20 cannot be done.

10. Can the following be the beginning addresses in CIDR based addressing?

144.16.192.32/28	-- YES ✓
10.17.18.42/28	-- NO X
188.15.170.55/28	-- NO X
200.0.100.80/28	-- YES ✓

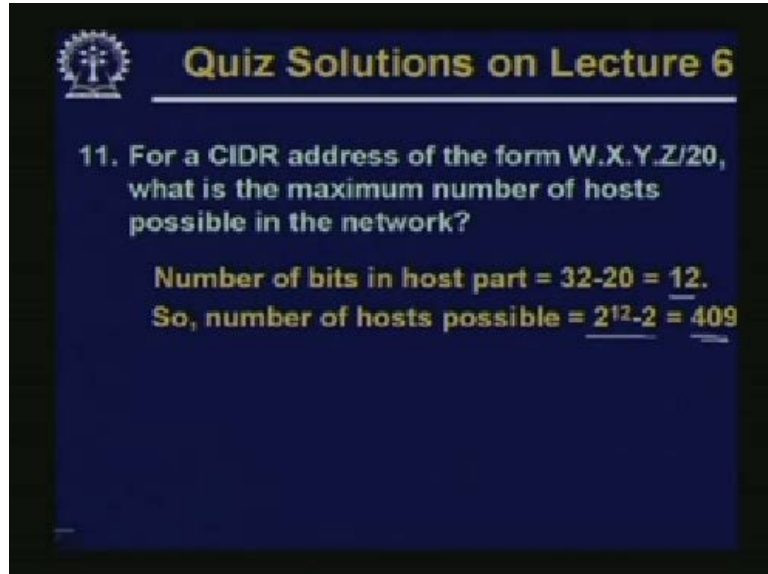
4
10000

Divisible by 16

If the number of hosts required are hundred 50, 50, 20 can VLSM be used. Well if you try to construct the same diagram, you will find that in the last step you cannot assign 50 and 20. So in VLSM you cannot use this because in the last step the sizes will be 32 and 32. Can the following be the beginning addresses in CIDR based addressing? See whenever you have 28 as the number of bits for the network or which means there are 4 bits in the host part, so the 4 bits must be 0 and if you keep a one before. This means 16, so the starting address must

always be divisible by the 16. So whichever address is divisible by 32 is divisible by 16, YES. 80 is divisible by 16, YES. But 55 and 42 are not. So these two cannot be the starting address.

(Refer Slide Time: 56:14)



Quiz Solutions on Lecture 6

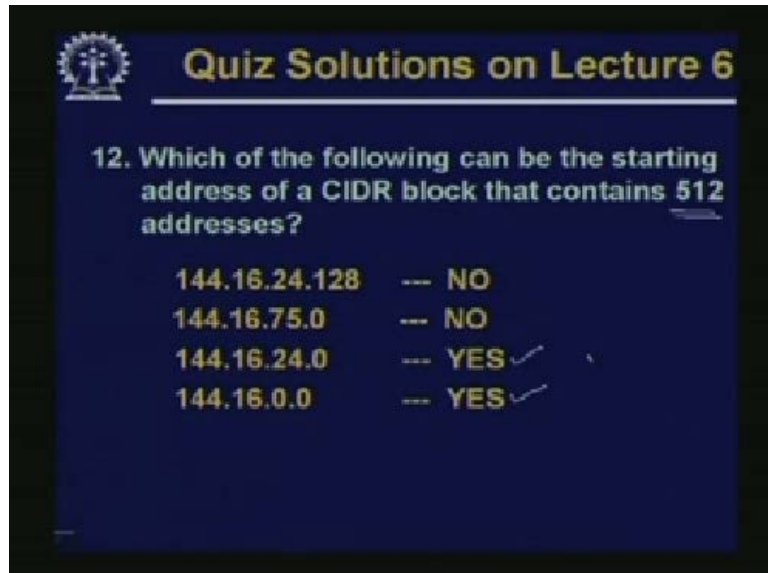
11. For a CIDR address of the form W.X.Y.Z/20, what is the maximum number of hosts possible in the network?

Number of bits in host part = $32-20 = 12$.

So, number of hosts possible = $2^{12}-2 = 4094$

For a CIDR address of the form W X Y Z/20, what is the maximum number of hosts possible? So number of bits in the host part will be 12. So the number of hosts possible will be 2 to the power 12 minus 2, 4094.

(Refer Slide Time: 56:34)



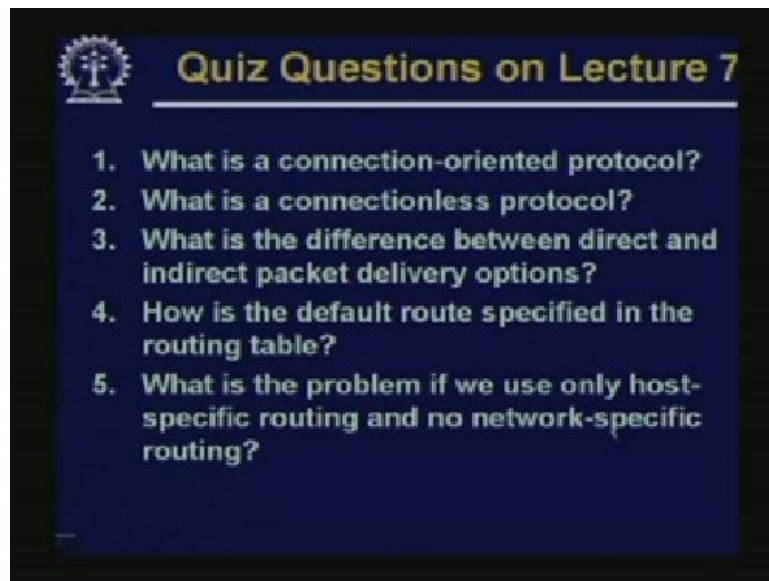
Quiz Solutions on Lecture 6

12. Which of the following can be the starting address of a CIDR block that contains 512 addresses?

144.16.24.128	--- NO
144.16.75.0	--- NO
144.16.24.0	--- YES ✓
144.16.0.0	--- YES ✓

So again, for a CIDR block that contains 512 addresses, which of these can be the starting address? You will see that which of the ones are divisible by that you can easily see just using the same principle I had used earlier that only the last two are possible. The first two are not based on today's lectures. Here are some questions.

(Refer Slide Time: 57:00)



What is a connection-oriented protocol?

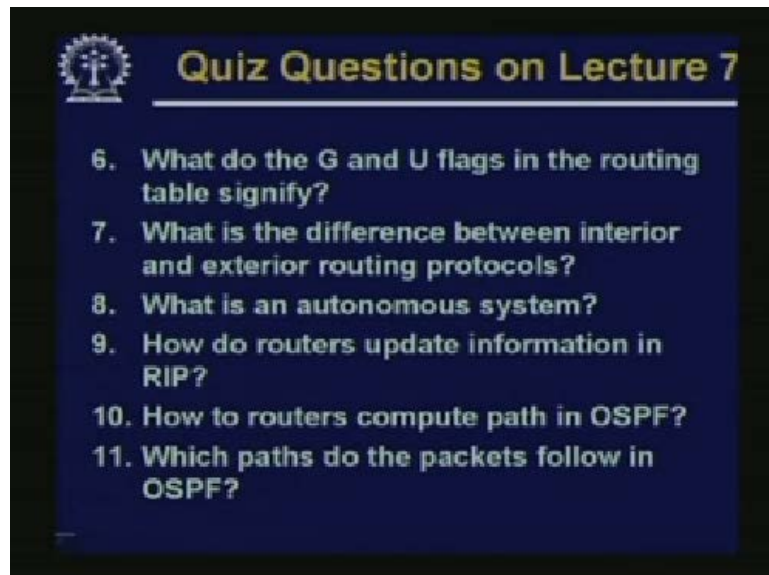
Number 2. What is a connectionless protocol?

Number 3. What is the difference between direct and indirect packet delivery options?

Number 4. How is the default route specified in the routing table?

Number 5. What is the problem if we use only host-specific routing and no network-specific routing?

(Refer Slide Time: 57:29)



Number 6. What do the G and U flags in the routing table signify?

Number 7. What is the difference between interior and exterior routing protocols? This we had mentioned so many times.

Number 8. What is an autonomous system?

Number 9. How do routers update information in RIP?
Number 10. How do routers compute path in OSPF?
Number 11. Which paths do the packets follow in OSPF?
So with this we come to the end of today's lecture. Thank you.

(Refer Slide Time: 58:07)



Preview of next lecture.

(Refer Slide Time: 58:08)



Internet Routing Protocols Part –II

In today's lecture, we would be continuing our discussion on Internet routing protocol. Shift to attenuation is a slightly different topic. Now if you recall when we had talked about TCP/IP earlier, we had basically talked about the IP version 4. We said that it is the most

commonly used protocol, that is been used in the network layer protocol in the internet. IP version 4 is basically a datagram base service which takes the responsibility of routing the datagrams from one source to a given destination. So each of the IP layers in the intermediate nodes, take decision, typically with respect to the IP address of the destination that means where to forward the packet to.