Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 11
Routing Protocols (Part I)

If you recall our discussion so far we have talked about the TCP/IP protocol suit, where if you recall, we have seen how packets flow through the Internet, through the network via the IP layer in TCP/IP, so that the packet can be forwarded or routed correctly from any source to any particular destination. Now, exactly how this routing or forwarding of the packet happens, these are dependent on something called routing protocols or routing algorithms.

There are networking devices as we had mentioned at the beginning called a routers which are primarily responsible for forwarding or routing of these IP packets ok. So, this is what we shall be starting our discussion with in this lecture. The lecture is titled Routing Protocols, the first part.

(Refer Slide Time: 01:17)

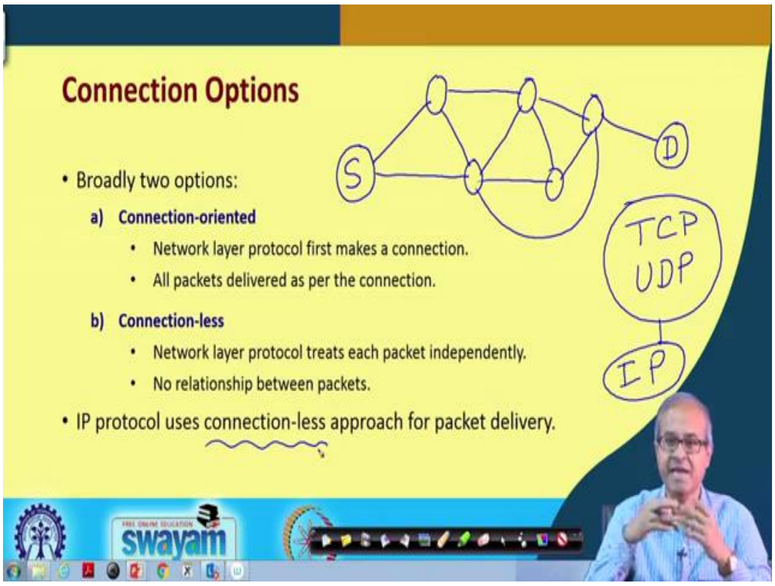
CONCEPTS COVERED

❑ Packet delivery options

❑ Routing Methods

Now, in this lecture we shall be broadly looking at two things; first we shall be talking about the different packet delivery options which are there, when a packet flows through the Internet and some of the alternate routing techniques or routing methods that are possible in this context ok. So, let us look at broadly the Internet routing protocols, how they work?

(Refer Slide Time: 01:47)



Connection Options

- Broadly two options:
  - a) Connection-oriented
    - Network layer protocol first makes a connection.
    - All packets delivered as per the connection.
  - b) Connection-less
    - Network layer protocol treats each packet independently.
    - No relationship between packets.
- IP protocol uses connection-less approach for packet delivery.

Before going into the routing protocols, let us talk about something called connection options. Now here what we are talking about is, suppose I have a source node which is trying to send some packet to a destination node. These may be computers connected to the Internet and there can be various intermediate nodes which in this context a routers through which the packets may flow ok. The source may be connected to one or more such routers and so, here I have shown two connections. For example, there can be a multiple such connections right.

Now, you recall when we talked about TCP/IP protocol suit, we talked about the two different protocols that are mostly used at the transport layer level namely TCP and the UDP. TCP is connection oriented UDP is connectionless. So, what it really means, let us again recapitulate connection oriented means, the network protocol whatever protocol you are using at the transport layer and the network layer level, must first be establishing so called connection. In TCP there is a connection establishment phase, we talked about using three way handshake ok.

Now, once connection is made, a pure connection oriented protocol says all packets are delivered as per the connection ok. You see here there is a catch, this statement does not mean that all packets will be following the same path. Connection is a logical concept.

When I say that I am connected with a destination, this means when I will be sending messages, receiving messages, I will be keeping track of my connection; that means, how many bytes have been sent; how many bytes are remaining to be sent?

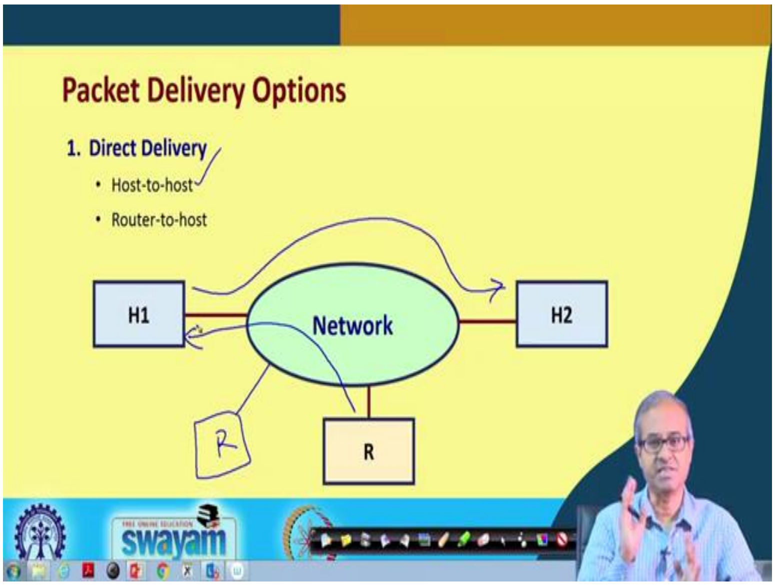
Similarly, for the other side also. So, it does not mean that when I am sending the bytes, they all will follow the same path. This would happen of course, when you are having something like circuit switching. In circuit switching you recall there all data will be following the same path. But when you are talking about a packet switch network like TCP/IP, there it does not happen like that. A logical connection is maintained at the TCP level, but at the IP, the packets can follow any available route.

So, this is what is meant by connection oriented and connectionless just like UDP or IP, connectionless means there is no need for a prior connection establishment. The data packets that you are sending, they are sent as independent entities. They will be routed through the network without any context in an independent way and they will finally, reach the destination.

Now, we mentioned that this UDP protocol which is a classical connectionless protocol, which is used at the TCP level, does not guarantee reliability in packet transfer. So, if you need reliability and if you are using UDP, you have to take care of error correction and this checking explicitly at your application layer level ok, fine. So, this is what I mentioned TCP and UDP are protocols at the transport layer level, but below it you have the IP protocol which runs at the network layer level which is essentially a connectionless packet delivery system, IP.

So, even if at the higher layer TCP talks about connection oriented, but when the packets are given to IP for actual delivery, IP can follow any path, arbitrary paths. So, this actually means that in the TCP protocol when the packets are sent between a source and a destination, packets may follow different paths. But the TCP protocol maintain some information about the connection such that the application has a feeling that well there is a connection, there is a reliable mode of connection, no errors are there, no bits are getting lost and data are being received exactly in order ok. This is what TCP provides over IP.

(Refer Slide Time: 06:50)



Packet Delivery Options

1. Direct Delivery
   - Host-to-host
   - Router-to-host

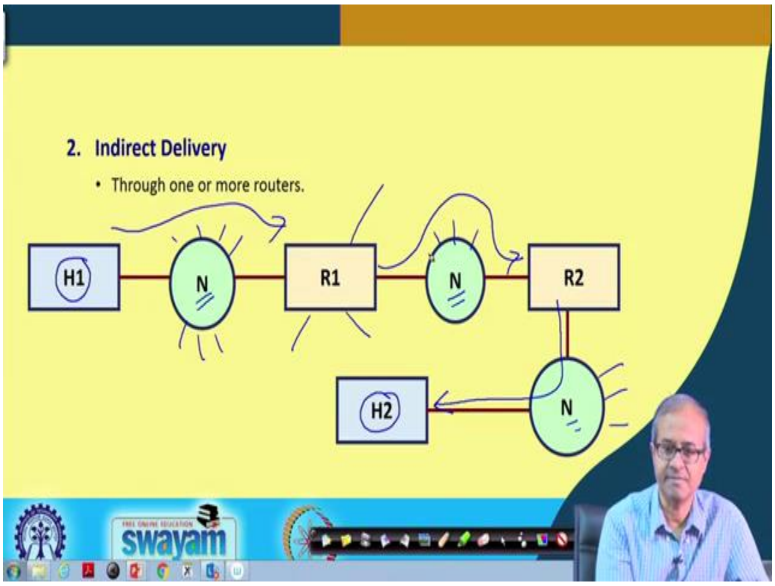
Now talking about the packet delivery options, I am particularly talking about the IP layer here, because as I said, TCP/IP is the most dominant protocol that drives the Internet and IP is the most widely used protocol at the network layer level which is responsible for packet routing. So, when you talk about packet delivery options, we are talking about a scenario like this as I have shown in this diagram.

There is a network as you can see in the middle, there is a network, there can be some computers which are directly connected to the network. You already seen, you have seen networks in your organization, in your office wherever you are. There are computer networks, there are networking switches or hubs and you have connection to your computer through these networking devices right. So, this hosts can have direct connection to the network and also there can be some routers; routers can also have connections to this network.

Now, the question is, in this network there can be multiple hosts H1, H2, two I have shown. There can be several others. So, all these hosts can communicate among themselves through this network. So, the question arises why do we need this router? This router is required when there is a communication need with other networks, whenever you want to communicate with the outside world. Well, either one of this hosts is trying to send a packet to some host which is outside this network or some incoming packet is coming from somewhere which is destined to one of these hosts. Now the first mode is called a direct delivery, where we are not talking about the outside world. We are talking about a scenario like this where this H1 can directly send a packet to host H2 via this network, because both of these are connected to the network, they have a connection. So, they can directly send a packet or receive a packet. This is called host-to-host.

And the other can be host-to-router or router-to-host, there can be one or more routers. One I have shown, there can be more routers connected, there can be other routers also connected. For example, there is another router here. So, router-to-host means suppose a packet has come to the router, the router can send this packet to a particular designated host or the other way around, host wants to send a packet to the router. Now, this direct delivery option is possible when the entities which are communicating, they are all connected to the same network. This is the constraint ok, this you should remember.

(Refer Slide Time: 09:53)



2. Indirect Delivery

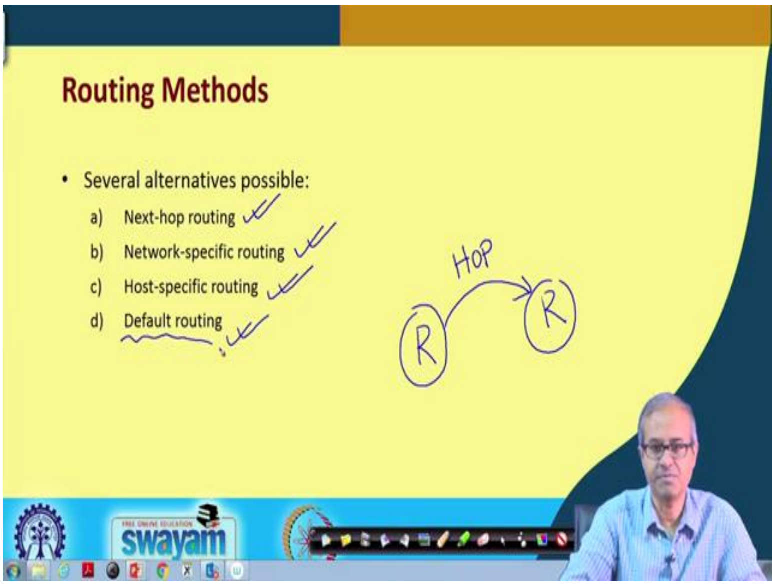
- Through one or more routers.

Then comes indirect delivery. Indirect delivery means the source and destination are not part of the same network. They belong to two different networks. So, as this diagram shows, let us suppose this H1 wants to send a packet to host H2. So, as you can see, there are three networks. Here, this N means networks. There are three networks, but I have shown only some, there can be other connections also to the network, other hosts and routers. There can be connections ok. So, I have shown only few.

Now, when this host wants to send data to H2, as you can clearly see, they do not belong to the same network. So, data cannot be sent directly. So, what will happen? Somehow H1 will decide that the packet that I am sending has to be sent to R1. So, it will first send the packet to router R1. The R1 can again have other connections, but R1 will decide depending on the destination address that this packet has to be forwarded via this network, middle network to another router R2 right and R2 will finally, come to know that well destination is in the same network where I am.

So, I can directly send the packet to H2. So, the last phase, it is direct delivery; in the first two steps, it is indirect delivery right. This is how packet forwarding and delivery can happen.

(Refer Slide Time: 11:35)



Routing Methods

- Several alternatives possible:
  a) Next-hop routing
  b) Network-specific routing
  c) Host-specific routing
  d) Default routing

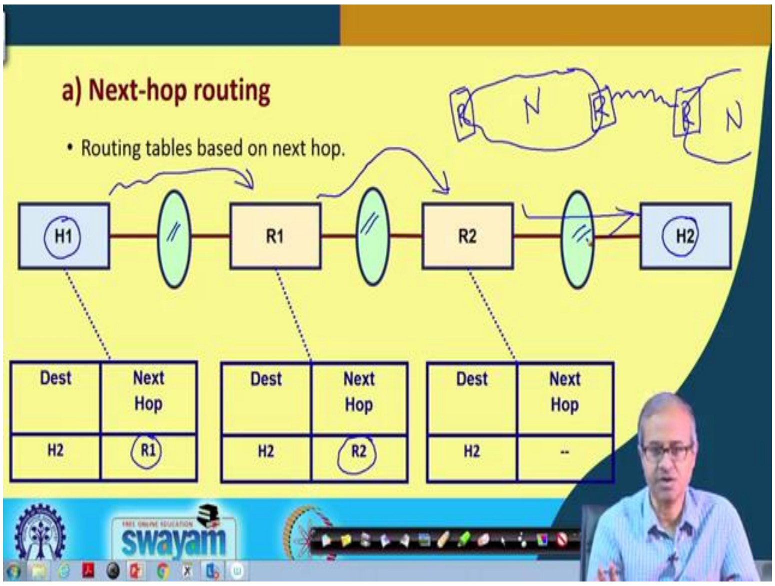
Now, talking about routing method, you see each entity in the network, routers of course, but even the computers, they have some kind of routing information maintained, that is called a routing table. Routing table will tell you that well if I want to send a packet to some other computer whose IP address I know, where to send that packet. Well, a router obviously, will be having multiple connection.

So, there is a decision, but even for a computer, it is possible for you to have multiple network cards and multiple network connections with your computer. So, your computer can also decide where to forward the packet. So, in a sense you can even make a normal computer act like a simple router. It can also take some routing decision, the IP layer of it.

Now, talking about the routing methods broadly speaking, the routing table contains various different kinds of entries, as you shall see through examples. They can be something called next-hop routing, network-specific routing, host-specific routing and default routing. Next-hop routing means I tell that to reach a particular host which is the next network or next router to follow that is called hop. One router to the next router, this is defined as a hop. So, when a packet moves there will be multiple such hops, till it reaches the destination network where the packet can be delivered directly ok.

Network-specific routing means there are some situations where you may want to transmit a packet to all hosts of a particular network. So, there you are not sending the packet to a particular IP address, but to a network as a whole. This is network-specific routing, you are specifying a network address as the destination. Similarly, you can specify a particular host that is called host-specific routing where to follow and if nothing matches in the routing table, there will be a default entry. If nothing matches, you take the default route. This is how typically routing tables are organized and these are the kind of entries which can be there fine.

(Refer Slide Time: 14:21)



a) Next-hop routing

- Routing tables based on next hop.

Dest	Next Hop
H2	R1

Dest	Next Hop
H2	R2

Dest	Next Hop
H2	--

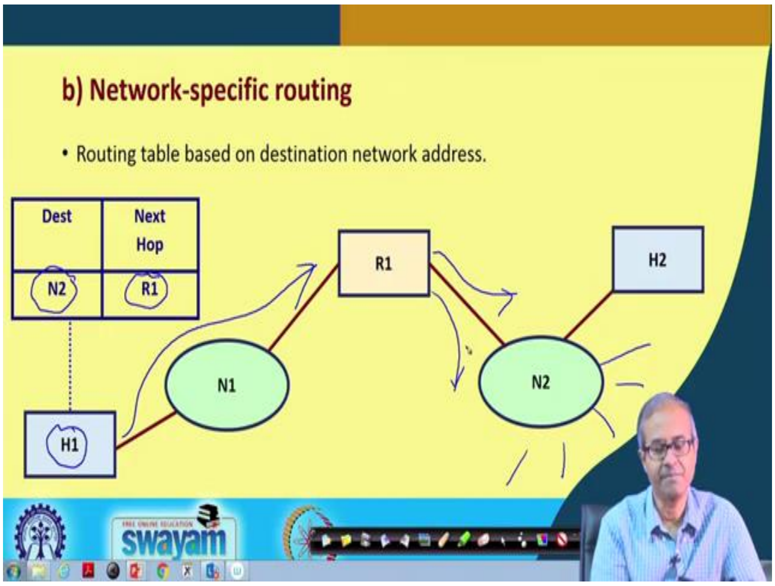
Now let us take some examples. Next-hop routing here, what we see here, again there is a scenario where a particular host H1 let us say wants to send a packet to another host H2. There are some intermediate networks through which the packets will be flowing and there are routers connected like this. Well, in this context let me tell you that in a practical scenario what happens? Suppose I have a network, this is a network ok.

There can be multiple routers which can be connected to this network and this, there can be another network for example here. There will be another router connected to this network and there can be a router to router connection like this. Normally connections are done like in this way, but here for simplicity I have shown that these routers are connected to networks. Networks are again connected to routers like that, but in an actual scenario the connections can be like this ok.

Next-hop routing what it says is that this destination as I said, each host, our computer will also have a routing table. So, there will be one entry in the routing table. Well, the most essential information routing table will contain is that if my destination is H2 what will be my next hop? Well, if I have to reach H2, my next hop will be R1. So, I will have to first send my packet to R1. This is a host to router, indirect delivery and in the routing table of R1, there will be something like this. It says again if the destination is H2, then I have to go to R2.

So, again this R2, this R1 router will be sending or forwarding the packet to router R2 and R2 has an information like this, it says H2, there is no next-hop means it belongs to my own network. So, now there can be a direct delivery right. This is what next hop routing is.

(Refer Slide Time: 16:50)



b) Network-specific routing

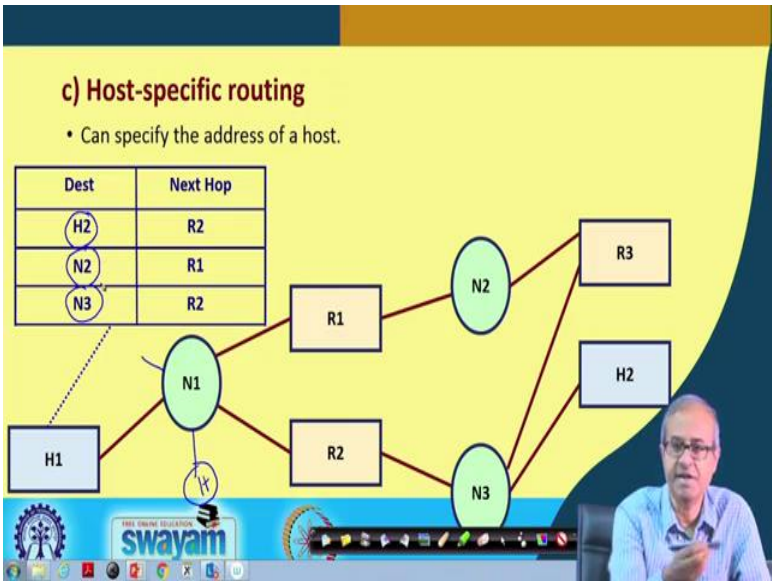
- Routing table based on destination network address.

Dest	Next Hop
N2	R1

Then network specific routing, I said sometimes I specify the address of a network as a destination rather than a, sorry rather than a host. So, I can specify the address of a network as the destination. So, suppose from host H1, I am sending a packet, I am specifying I have to go to N2. It can be a broadcast packet, it will be broadcast to all the hosts in N2.

So, here again similarly I can specify the next hop as R1 which means if I have to go to N2, then first the packet has to be forwarded to R1. Similarly, R1 will be having a routing table that routing table will say that well N2 is, I am a part of N2. So, I can directly do the broadcast whatever is requested ok. This is how it works.

(Refer Slide Time: 17:56)



c) Host-specific routing

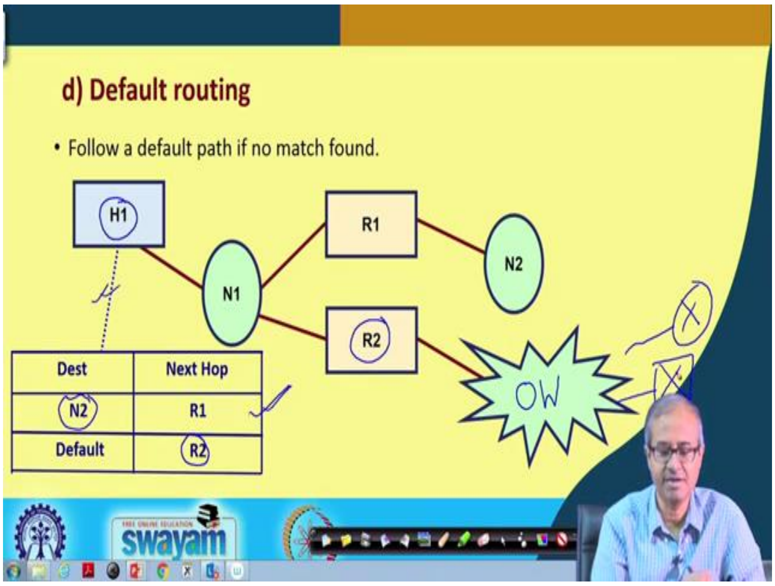
- Can specify the address of a host.

Dest	Next Hop
H2	R2
N2	R1
N3	R2

And lastly, host-specific routing means in the destination I can directly specify a host and this host can be connected to the same network also. There can be some other hosts connected here also. So, host specific routing means well of course, next hop will be, they are very similar. So, it is actually quite similar, not something which is very different; the only difference is that in the destination I specify the complete IP address of a host ok. So, that is referred to, sometimes refer to as hosts specific routing, where we specify the IP address of a host.

So, let us say if I want to go to H2, I have to go through R2. If I want to go to N2, I have to go via R1. If I want to go to N3, I have to go via R2. So, this kind of entries are there. So, it is mixture of, some are host-specific routing entry, some are network-specific routing entry like this. So, when you look at the complete routing table of a typical router, we shall see later, then we will see that all these types of entries are all there.

(Refer Slide Time: 19:14)



d) Default routing

- Follow a default path if no match found.

Dest	Next Hop
N2	R1
Default	R2

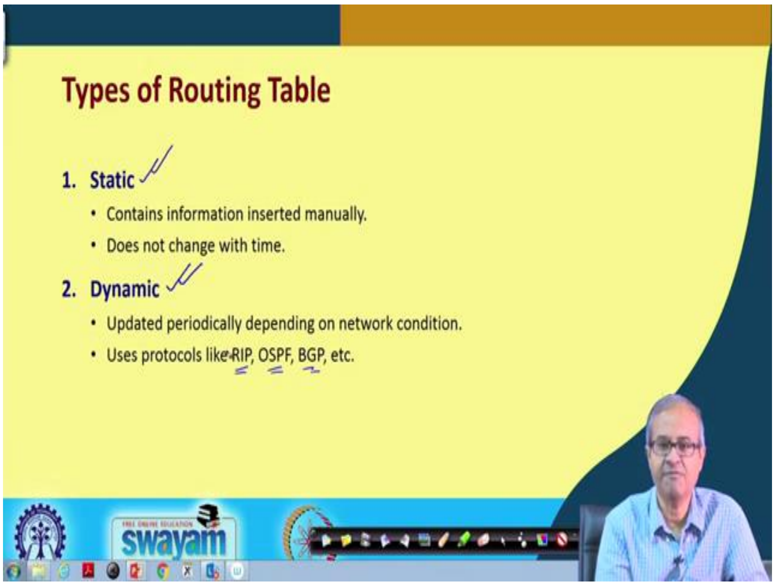
Now, lastly I said whenever nothing matches, you have to follow a default route like you take an example like this, where I have a host H1 here. This H1 wants to send some data to some host, other host which is somewhere else in the world, not in this network, it is somewhere else right. So, it does not know where it is.

You see in the world there are millions of computers, it is not possible for me or my router to know where all these million hosts are located, it is not possible. So, what it will do? There will be some entry, well here I have shown only one, which are specific to the local network. Well, if your destination network is N2 which this routing table is aware of H1 knows, then you will forward it to R1, through R1 you can reach N2.

But if it does not matches, what we will do? If it is something else which is not N2, then you will be following the default route, it says if nothing matches you have to go to R2 and R2 is a router which is connected to the outside world. This is your outside world; that means, this is an external connection from your organization, you are connecting to the router of maybe your Internet service provider or some other organization that router will then be responsible to forward your request to the correct direction ok.

This is how it works. You will be forwarding this packet to this R2 and R2 will be forwarding it to the outside world, maybe to some other router, to some other router who is more knowledgeable, who knows where to forward, this called higher level router right. This is default routing.

(Refer Slide Time: 21:22)



Types of Routing Table

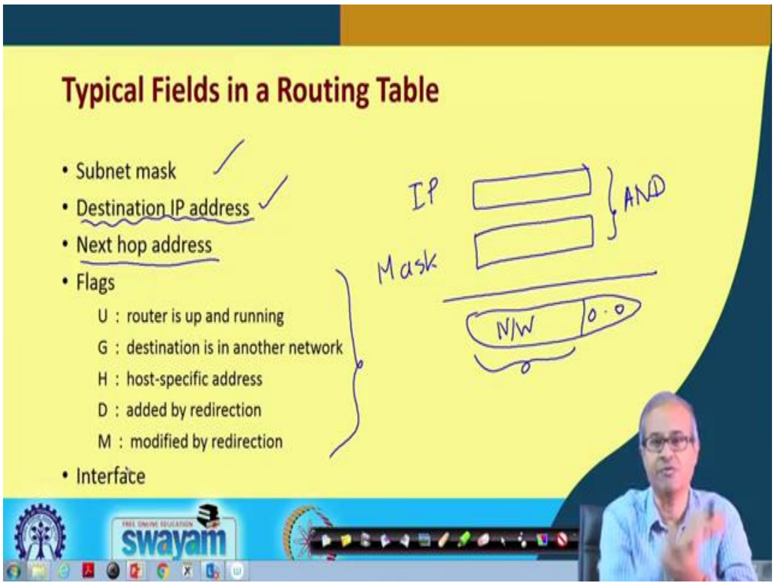
1. **Static**
   - Contains information inserted manually.
   - Does not change with time.
2. **Dynamic**
   - Updated periodically depending on network condition.
   - Uses protocols like RIP, OSPF, BGP, etc.

Now, talking about the types of routing table, some entries in the routing table are created manually, they do not change with time ok. You know this structure of your own network; you know how the machines are connected, how many routers are there. So, you can make some entries in the routing table which will never change that is fixed. These are called static entries. Typically, these static information will be entered manually by the network administrator which does not change with time normally.

But more practical situations, we will see some dynamic updates happening in the routing or in the routing tables because you see network is large. So, when with time whenever packets are flowing, there can be some dynamic behavior that may happened like some link might go down, some host might be come down. So, some path which was there might no longer be available. So, this router should be intelligent enough to find an alternate path if such an untoward incident happens. There this dynamic behavior comes into the picture.

So, dynamic routing table, what they do? They carry out some updations in the routing table automatically with time, updates periodically depending on the network condition ok. If a link goes down, in the future again the link comes up, you will have to make changes. There are protocols, we will be briefly talking about RIP, OSPF, BGP, they handle this kind of dynamic updations.

(Refer Slide Time: 23:14)



Typical Fields in a Routing Table

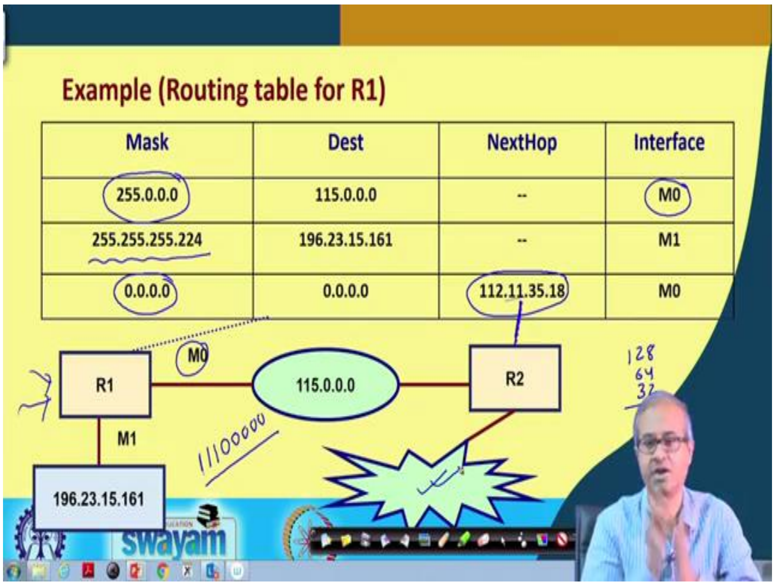
- Subnet mask
- Destination IP address
- Next hop address
- Flags
  - U : router is up and running
  - G : destination is in another network
  - H : host-specific address
  - D : added by redirection
  - M : modified by redirection
- Interface

Talking about the typical fields in a routing table, well you already know what is meant by an IP address and a subnet mask. This routing table contains an IP address and also a subnet mask. This is an IP address and this is a mask, both will be 32 bit quantities. So, I mentioned earlier to get the network address, you will have to do a bit by bit AND operation. You will have to carry out a bitwise AND operation. So, once you do a bitwise AND operation, what you get, will be your network number and the host portion will become all 0’s ok.

Based on this network number, you will now be, take a decision that if there is a match where to go ok. So, we will see with respect to IP, you first apply the mask, then you compare whether there is an IP address field or destination address field in the routing table; whether this network number matches with this destination? If it matches, then you follow the next hop address what is specified and there are some flags which are maintained in the routing table, which keeps track of few information.

Like the flag U indicates that router is presently active, it is working. G means that this is an indirect routing, destination is not in the same network; it is in this some other network, which means you will have to forward it to one of the routers. H means you are giving the complete IP address of a host, it is a host specific address and D means this entry was not there initially due to some dynamic updates, this new entry got added to the routing table. This and M means there was an entry, but there was some changes made in the entry because again due to dynamic updates. So, this is modified, this is added; both due to this dynamic updates or redirection and of course, an interface information, the router, kind of multiple outgoing links which link to follow that is called the interface.

(Refer Slide Time: 25:57)



Example (Routing table for R1)

Mask	Dest	NextHop	Interface
255.0.0.0	115.0.0.0	--	M0
255.255.255.224	196.23.15.161	--	M1
0.0.0.0	0.0.0.0	112.11.35.18	M0

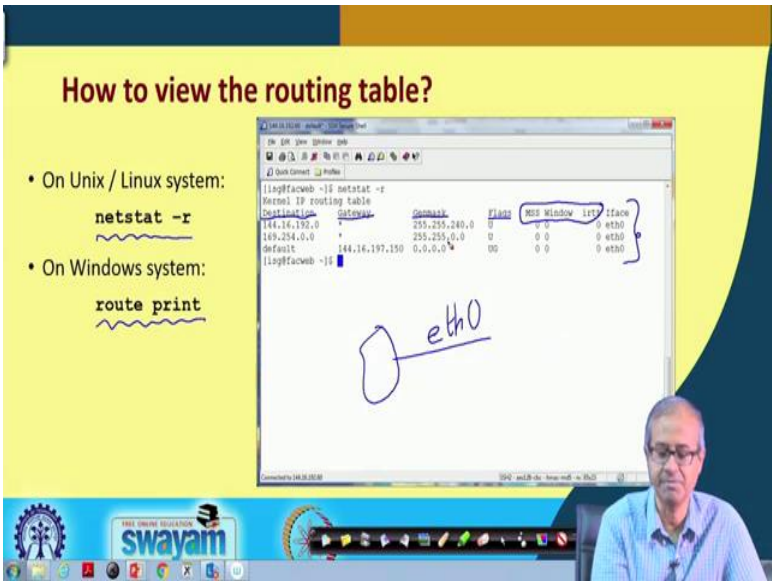
So, this is one simple example of a routing table which is slightly elaborated here. You consider a network like this, where you see this is a network whose network address is 115.0.0.0.

This is a class A address, class A network and there are two routers R1, R2 connected to this lets say and one computer whose IP address is this, 196.25.15.161 is connected to this router let us say, just an example and this router R1, this routing table I am showing, this is for the router R1 ok. For this router R1, you see three entries are shown; first says I use a mask of 255.0.0.0 which means only the first 8 bits will remain, if I do a bit by bit AND, the last 24 bits will all become 0’s.

So, if there is a packet coming to this router R1, maybe from this host or any other host, it will first do AND with 255.0.0.0 and compare if the network address is equal to 115.0.0.0 or not, if so, it will send the packet to interface M0, its a directly connected. Through this interface M0, it will directly send it to this network ok. Similarly, if an incoming packet here the mask is 255.224. 224 means what? 128 see 128 and 64. This is 192 and 32 this becomes 224. So, the last byte is 111 and five-zeroes this is 224 in decimal.

So, whenever an address comes, you do a bit by bit AND with this and then, you compare whether it is matching with this. If it matches, then you forward it to M1 and if nothing matches, 0 means default; 0.0.0.0 entry means default. If it is default, then you go to here this. This is the IP address of this router R2 ok. This is the IP address of this router R2. If nothing matches the packer will be sent to R2 and R2 will send it to the outside world and the packet will ultimately find its way. This will be done through interface M0 again fine.

(Refer Slide Time: 28:51)



How to view the routing table?

- On Unix / Linux system:

  netstat -r

- On Windows system:

  route print

```
[isg@facweb ~]$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
144.16.192.0    *               255.255.240.0   U         0 0          0 eth0
169.254.0.0     *               255.255.0.0     U         0 0          0 eth0
default         144.16.197.150  0.0.0.0         UG        0 0          0 eth0
[isg@facweb ~]$
```

Now, the question is in a computer or in a router how do we view the routing table. Let us say on a computer if you are, if you are using a Unix or a Linux system, then the most command to use is “netstat – r”. Similarly on an windows system there is a command called “route print”. It will print the routing table of that computer. Like in this screen, well the entries are very small, you may not be able to read clearly.

So, I have given “netstat – r” command and you see the routing table, there are three entries in the routing table which show up, it contains Destination; Gateway means the next hop; Genmask this is the subnet mask; Flags and some other TCP related information. This MSS means Maximum Segment Size, window means TCP window and RTT means Round Trip Time; some information regarding to that and this is the interface, which interface?

Now, here I am assuming that my computer is connected to only one interface, this is called eth0 ok. So, this is how you take a decision and you say flags are u, u and g; u means they belong to the same network and g means it belongs to the other network right. So, this is just an example, I have shown. So, with this we come to the end of this lecture. In this lecture, we have had very brief idea regarding the routing of IP packets and how the IP routing table looks like.

Thank you.