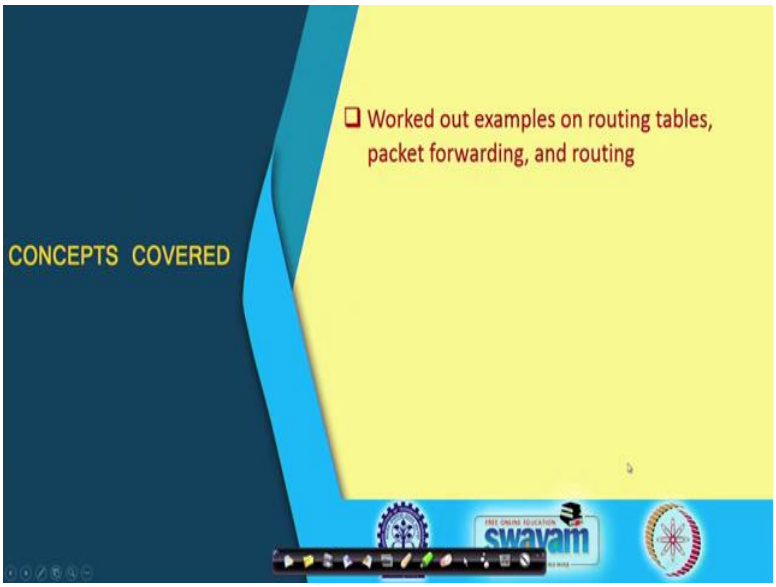
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 15
Routing Examples

In the last few lectures, actually we have discussed a number of so called routing algorithms which help an IP packet to traverse from a source to the destination through a number of intermediate routers. We talked about two classes of inter router protocols; the interior and exterior so called routing protocols which help the routers to update their routing tables in a dynamic way.

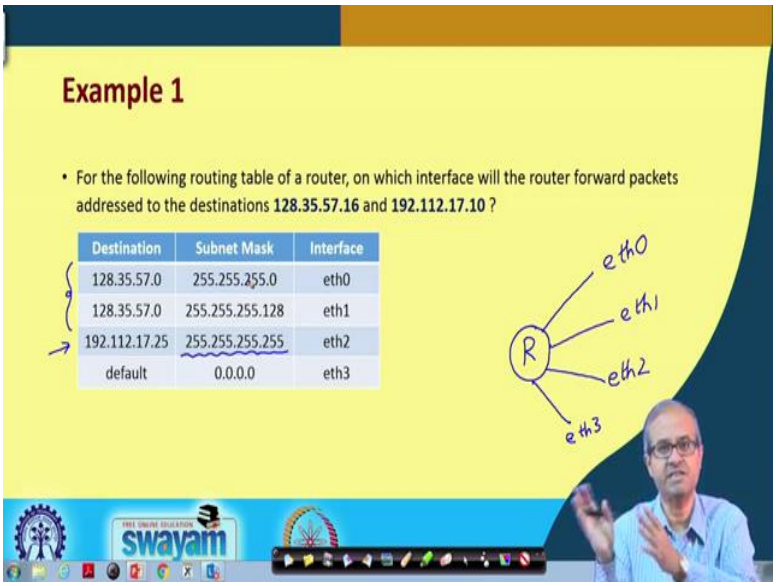
Today we shall be looking at some examples, where we shall see that given a certain routing configuration in the form of a routing table, whenever a packet comes with a particular destination address, how the packet is handled, how it is forwarded to the correct outgoing link of that router. So, the topic of today's lecture is routing examples.

(Refer Slide Time: 01:17)



So, as I have said in this lecture we shall basically be working out some examples that will involve routing table and packet forwarding and in general routing of IP packets. So, let us get started.

(Refer Slide Time: 01:34)

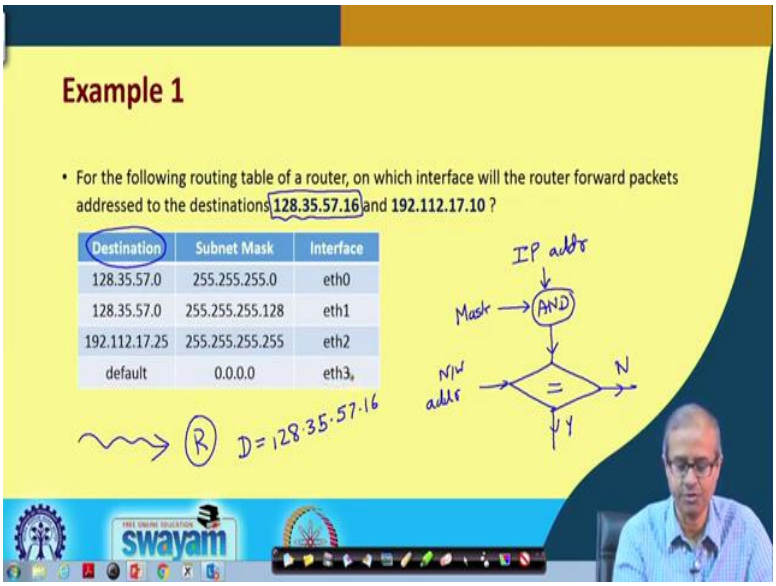


The first example that we take here, is something like this. Let us assume that we have a router, let us say we have a router which has four interfaces. There are four links to the router and this interface names we are giving as eth0, eth1, eth2, eth3. Now this eth is the short form for Ethernet, because typically inside a LAN this interfaces are typically Ethernet networks, so that is why we are giving this names like this eth0 to 3.

Now, you look at this routing table. Well here I have not shown all the fields, the relevant fields only I have shown, destination IP address or the destination network address, subnet mask and which interface to forward it to. So, you see there are four entries, there are four destination network or host address.

You see the first two entries refer to network address, it starts, it ends with dot 0, but the last one is a host specific address. Because it is the host specific address, I am using all bits to check, subnet mask is all 1s, but for the others, subnet mask will tell you how many bits in the address I have to check for the network address and the last bits will be for the host address.

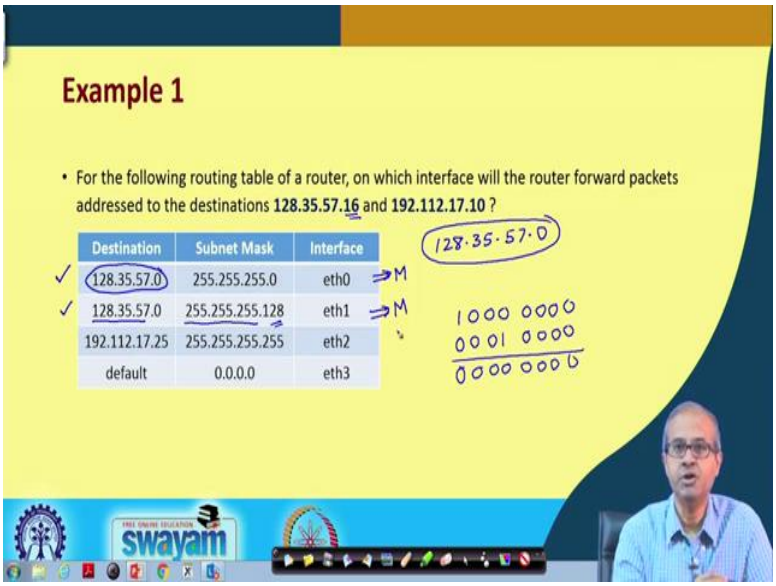
(Refer Slide Time: 03:27)



So, let us see, now the question is, there is an IP packets in the first example here, there is an IP packet which comes to the router, this was the router and an IP packet comes here, where the destination address is given by this 128.35.57.16. This is the destination IP address. Now we have to check which entry in this routing table are getting a match. There may be one or even more than one entry where there can be match as we shall see through this example. So, here what we do? The rule is as follows. We have the IP address, this we already mentioned earlier. With the IP address we do a bit by bit AND with the subnet mask whatever is specified.

And whatever you get after doing this ANDing, this we compare, whether it is equal to the network address or the host address which is specified in the network table, routing table. Here it is this destination field. So, if there is a match yes, then we follow the outgoing interface, but if there is no match, we do not find any match anywhere then we will be taking the default route, it will be forwarded to eth3 right. Now let us see. Now this 128.35.15.16 this will be checked with the rows one by one. First, this row, just look at it the subnet mask says the first three bytes are all 1s, last one is all 0, 255 means all 1's.

(Refer Slide Time: 05:18)



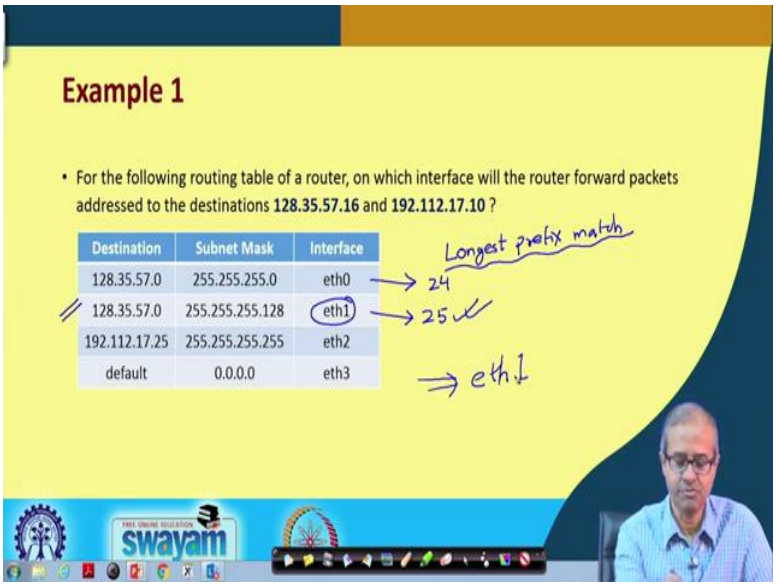
So, if you do a bit by bit ANDing with this, you simply get 128.35.57, last 8 bits will become 0, because you are ANDing with eight 0's at the end. Now if you compare this with the destination address out here, you see that there is a match right, this is exactly the same as this. So, in the first row you get a match, but in the routing table you do not stop here.

You also check the other rows, I will tell you why, first row there is a match all right. Now you similarly go to the second row, do a similar checking. Now you look at the subnet mask first three are all 255 alright, last one is 128.This 128 means a single one in binary followed by seven 0's. Now this will be ended with the last byte or octet, this is 16 ok.

Now, 16 is what? 16 is 00010000. So, the first three are all right, first three will be the same, if we ANDed with 255.255.255 it will be 128.35.57, but the last one, the 16 will get ANDed with 128.If you do bit by ANDing you see all are 0s. So, here again you will be getting the same thing; 128.35.15.0.

So, here also there is a match, there is a match in both the entries in the table, but for the third one, there will be no much as you can see, you are checking for all the bits, so the entire thing remains and this is certainly not the same as 192.0, so it will, there will no match. So, now you have a situation where there are two matches in the routing table.

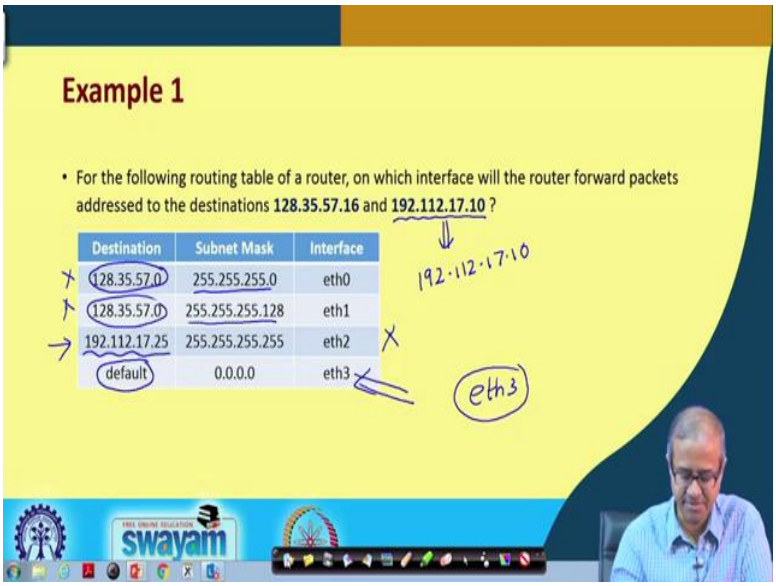
(Refer Slide Time: 07:40)



Now, when there are multiple matches in the routing table, the rule that is followed is, there is something called longest prefix match, longest prefix match, this is what you look for. You see in the first row there was a match, but how many bits was checked for the network address; first 8, 8, 8, 24 bits.

So, the network part was 24 bits, but for the second subnet mask, there were 24 plus in the last one, there was a single one, so it is 25, 25. So, you will always take the highest one, the longest network number for which a match is found. So, it will be considered that for the second entry the match is found and this packet will finally, be forwarded to eth1 interface right. So, this is how forwarding will take place for the first one. Let us look for the second one now.

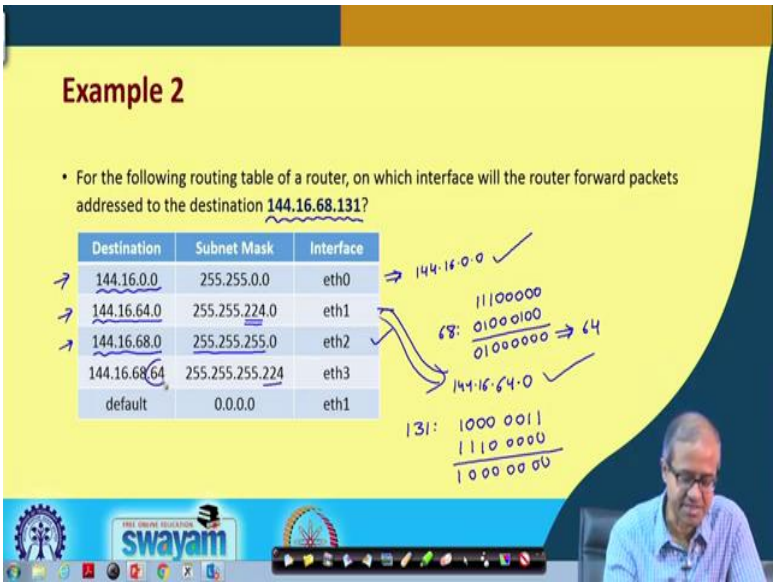
(Refer Slide Time: 08:51)



Well for the second one; obviously, the first two will not give match, because you are ANDing with 255.255.255. So, 192.112.17 will be getting anyway, but the destination starts with 128. So, there will be no match here, there will be no match here, so let us look at the third entry. So, you are checking for all the bits; that means, you are ANDing with all 1s, if you AND with all 1s, the same thing will remain, there will be no change 192.112.17.10.

So, now, if you compare it with this destination address also it is not matching, here this 25, here this 10, so here also there is no match. So, in that case, you will have to take the default route and this packet will be forwarded to eth3. This is how the packets forwarding will take place right ok.

(Refer Slide Time: 10:03)



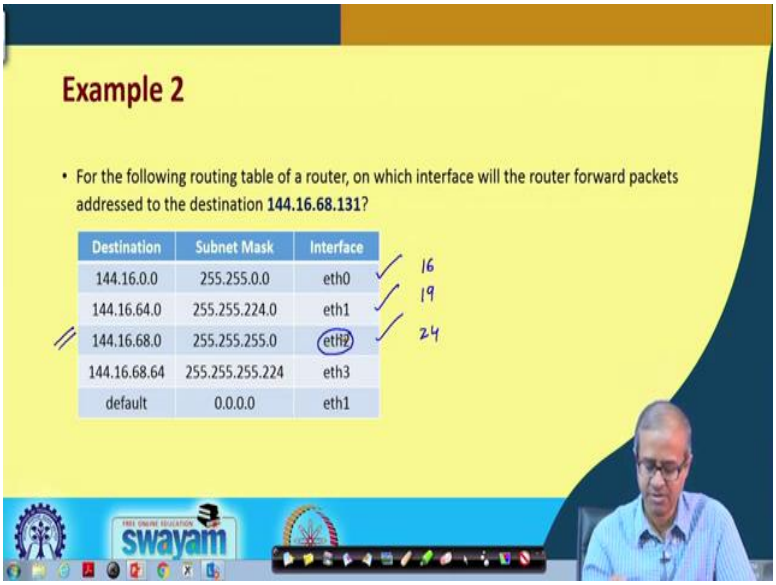
So, let us move on to the next example, this is a very similar example. Here I have assumed that the routing table is given, here there are five entries and here again an IP packet is coming whose destination address is 144.16.68.131. Let us look one by one where the matches are coming, let us take the first one. The subnet mask is 255.255.0.0, the last two bytes are all 0, so the last two bytes will become 0.

So, for this one, so after this bit by bit ANDing you will be getting 144.16.0.0 which is actually matching with this, so for the first one you will be getting a match. Let us look at the second one. For the second one, you see the third byte of the mask is 224.Now actually what is 224? 224 is nothing, but 111 followed by five 0s, this is 224. So, you will be doing a bit by bit ANDing of 68 with 224.What is 68? 68 if you convert to binary it will be 01000100, 64 and 4, 68. So, if you take a bit by bit ANDing, here what you get is, 0. This 1 and 1 will be 1000000 which in decimal is64, this bit is 1.

And the last one is 0, so 0, if we AND with 131, this will be 0 anyway. So, here also if you do an ANDing, it will become, this will come to 144.16, the third one will become 64, the last one will become 0. So, you see the destination address is exactly that, so here also there is a match. So, there is a match in the first two rows. Let us come to the third row; 255.255.255 all three. So, the first three 144.16.68 will remain, last one will become 0 which is the same as here. So, here also there will be a match. So, there is a match in all three rows of the table.

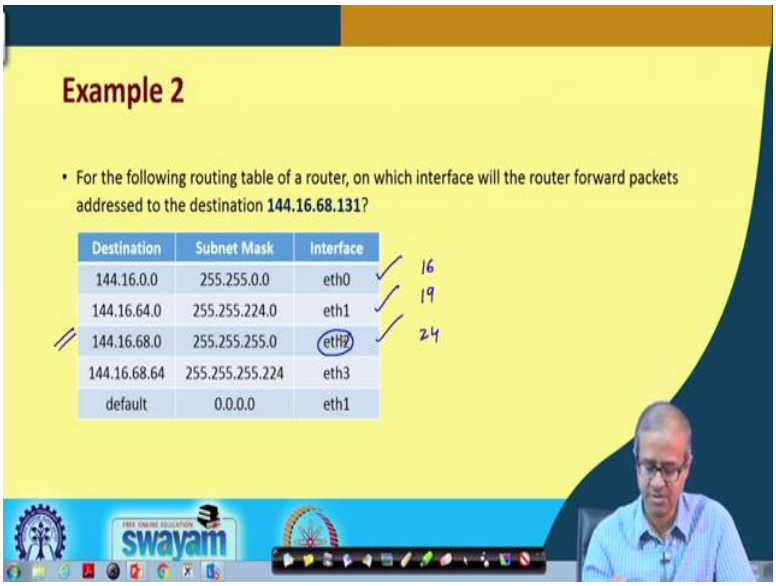
The fourth one you can check, here of course, there will be no match, because the first three 255.255.255, 144.16.60, this will remain and this 224 will get ANDed with 131. Now this if you do 220 say, 131 is what,131 is 128 plus 3, this is 131. So, if you do a bit by bit ANDing with 224, 224 is 111 followed by all 0s; so, only the first one will be 1, rest all will become 0s, this is 128, but here it is 64, so it is not matching right.

(Refer Slide Time: 13:42)



So, there is a match in this example for the first three rows. So, now, as I had said in router we follow the longest prefix match rule, you see with respect to the subnet mask, the first row had 16 bits of the network 255.255, second one had 16, 16, and 3, sorry 8,8 and 3, 19 and the third one had 8, 8 and 8, 24. So, the third one is the longest prefix. So, ultimately the match will be identified for the third row and the packet will be forwarded to this eth2 interface right, this is how the packet forwarding will take place.

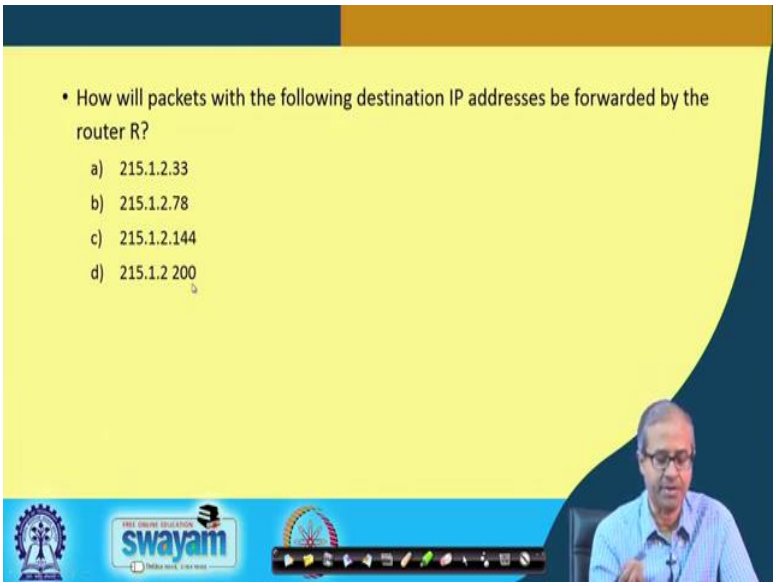
(Refer Slide Time: 14:28)



Now, let us look at a third example where here we are using subnets, sub networks. So, you see pictorially the network configuration looks like in the diagram as shown here, this is the router, we are interested in the routing table that we are showing here. This is the routing table of this router and this router is connected to four sub networks a, b, c, d through these four links small a, small b, small c and small d, and there is an exterior router which is connected to the outside world.

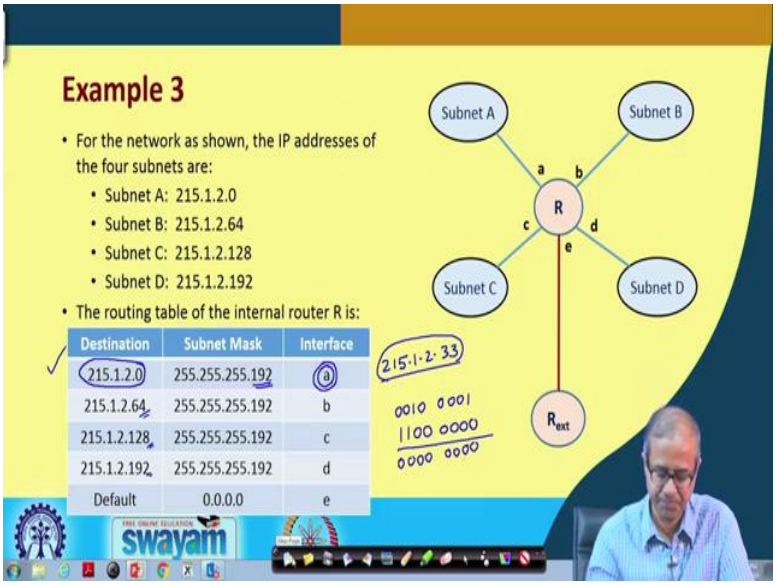
There is another fifth link e which is connected to that exterior router, this is how the connections are. Now we are assuming that the subnet, sub network addresses, the network addresses are as follows; this, this, this and this. They all start with two 215.1.2, the last eight bits are sub networked. So, you see 0 and 64 is the first one, it starts with the last byte 0, it continues till 63, b similarly it starts with 64 and continues till 127, the third one starts with 128 and it will continue till 191 and the fourth one will start with 192, it will go till 255. Now here suppose some packets are coming.

(Refer Slide Time: 16:19)



Let us go to the next slide. So, here we will work out this examples for these four packets, these are the destination addresses and we will try to find out what will happen. In the first one the last byte is 33, 78, 144 and 200.

(Refer Slide Time: 16:37)



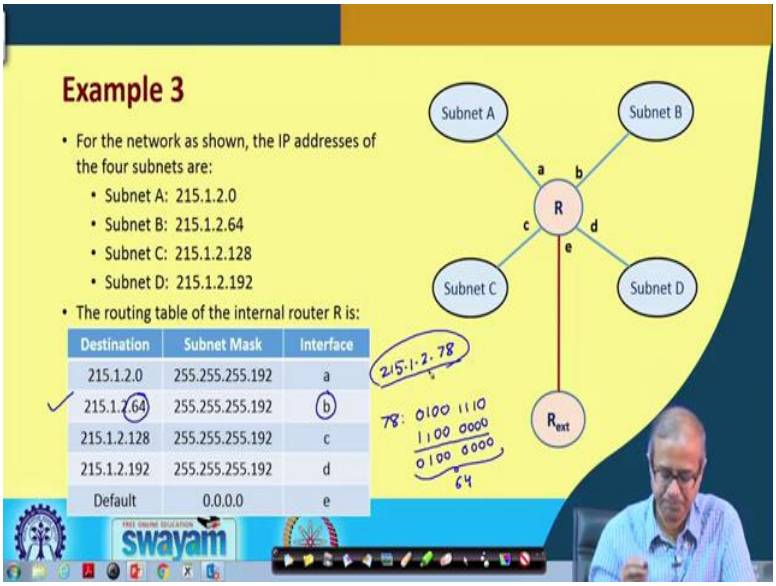
Now, you see logically speaking you can, now you can identify that said the first one will belong to the range of sub network a I mentioned 0 to 63, second one will be in b, third one will be in c, third one, fourth one will be in d, but let us see how according to this

ANDing and comparison this decision is validated. So, the first IP address which is coming, it has an address 215.1.2.22.

Now, you see let us make a check in this routing table one by one, if a subnet mask of all of them are 192 in the last one. Now what is192 ?The first two bits one, rest all are 0. This is 192. Now this 33 we will have to AND with this, what is 33? 33 is 0010 and 0001, 32 plus 1.If we do a bit by bit AND, it will become 0000000, all 0s. So, the last byte will become 0. So, you see, there will be a match with this 215.1.2.0. So, in the first row, there is a match. Just let us look at the second row, what happens? second row has 64 here.

The mask is the same, because we are getting 0, there will be no match, this is 64, third row also 192 same thing, this is 128, this is 192, so there will be no match in any other rows. So, this first packet will get a match with the first row and it will be forwarded to interface a, this is for the first packet right.

(Refer Slide Time: 18:47)

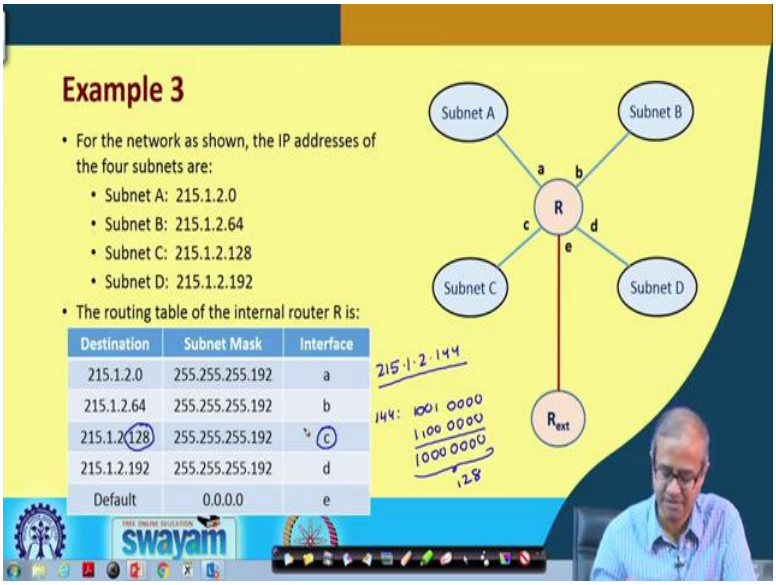


Let us look for the second packet now. this second packet had an address 215.1.2.78. Now what is 78 in binary? 78 in binary is 01001110. Now if you do a bit by bit ANDing with the mask, again 192, 192 is this. So, you see this second bit would be 1, 1 and 1, this bit will be 1, all rest will be 0s.

So, how much is this, in decimal this is 64. So, if you do a bit by bit ANDing with 192, it is 64, and if you look at these rows, there will be match only with this second one, because

64 is here. So, there will be a match with the second row and the packet will be forwarded to interface b ok, this is for the second packet.

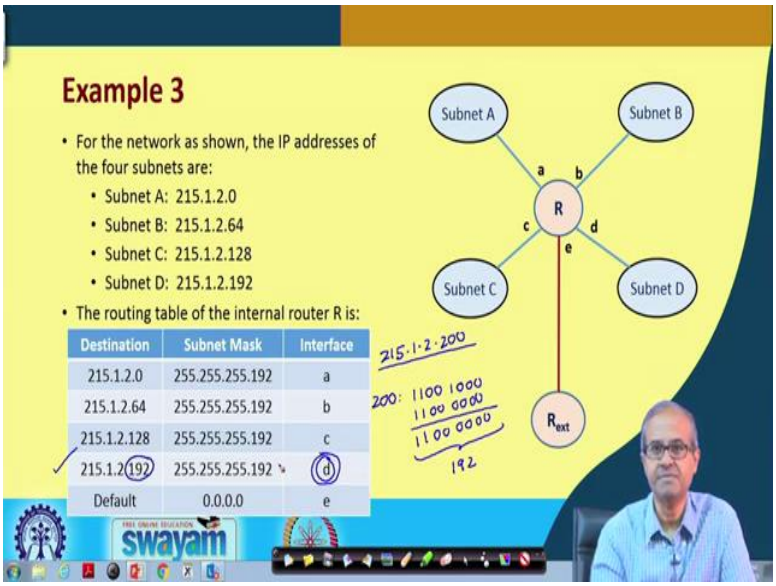
(Refer Slide Time: 19:58)



Let us look at the third one, the third one had an IP address of 215.1.2.144. Now let us do a similar exercise, what is144 in binary? 144 is 10010000 and this 192 as I had said, is 11000000.

If I do a bit by bit AND, 10000000 which is 128. So, there will be a match with the third row right and the packet will be forwarded to interface c fine ok.

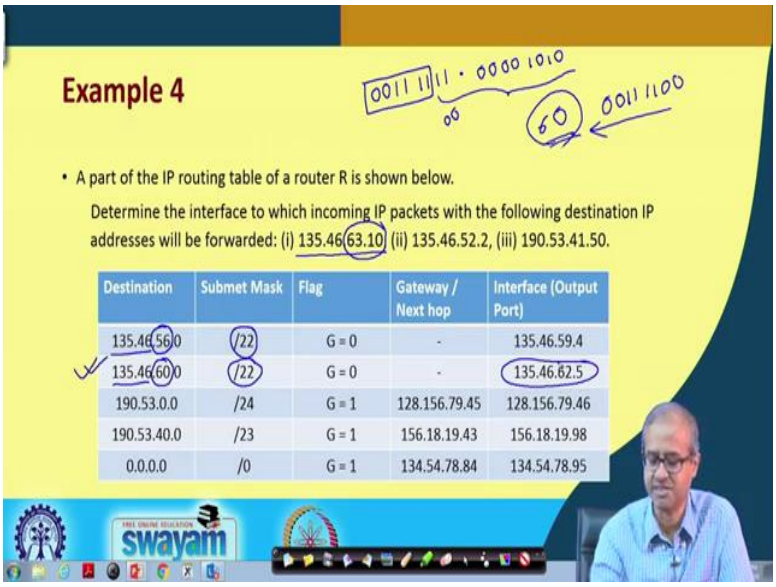
(Refer Slide Time: 20:51)



And the last one, the last packet had an address 215.1.2.200. Now similarly what is 200? 200 in binary is 11001000 and 192 is this. So, if you do AND, it will be 11000000 and 1100 hope in decimal, this is 192. So, there will be a match with the fourth row, there will be a match and the packet will get forwarded to d right.

So, this is how the packet forwarding is happening for this example.

(Refer Slide Time: 21:48)



Let us look at a fourth example. Now in this fourth example what we have done, here we have shown some additional entries in the routing table, more like a practical routing table and also we have shown the subnet mask in the CIDR notation. So, in many router when you see the routing table, the mask will be shown in the CIDR notation. So, here it is done like that.

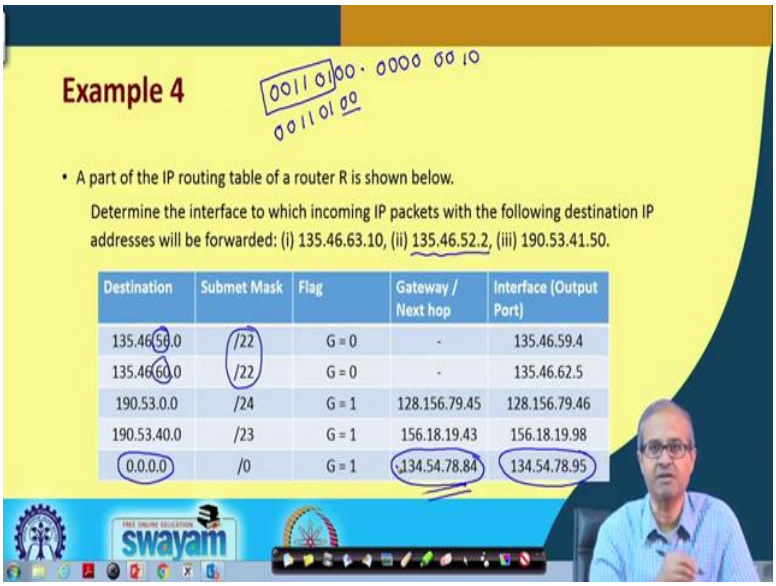
So, here we are actually talking about three such IP addresses destination, let us look at it. The entries what they mean, destination, subnet mask you understand and in the interface instead of some names; like a, b, c, d, e or eth0, eth1, some IP addresses are specified. These are the IP address of the output ports where the packet will be forwarded and gateway next hop is another column, I am just showing here, this means something like this.

Suppose I am considering the routing table of this particular router. This router may be connected to some other network, that network may be having some other router, there may be multiple outgoing links. Now if the destination is directly connected, you send it over the outgoing link, but if not, you will specify that this packet has to be sent to this some other router; that is the address of the gateway or the next hop.

So, you can specify the next hop address, also here as an optional choice. So, let us see, so for this particular address what will happen. The subnet mask says how many bits to be considered, so135.46.8 and 8.16. So, I am not worried about the first two, because 135.46 I can see, the first two entries already have. I only look at the last 2, 63 and 10. So, what is 63 and 10? 63 is 00111111, this is 63 and 10 is 00001010 and we are saying we will be looking at 22 bits of the address; first 8 and 8, 16 and 6 more. So, from here you take 6 more bits.

So, how much will it become, this will become if you do a bit by bit ANDing, these two, these will be host part, so these two bits will become 00. So, it will actually become 3, it will become 60, it will become 60. So, you see in the first entry, it is 56, so it is not matching 00111100, this is 60, 111100 this is 60. But in the second entry here also we are looking at 22 bits, but here it is 60. So, for the first example there will be a match found with a row 2, row 3, row 4; obviously, there will be no match because they are starting with 190. So, the first packet will be forwarded to this particular interface right.

(Refer Slide Time: 25:46)

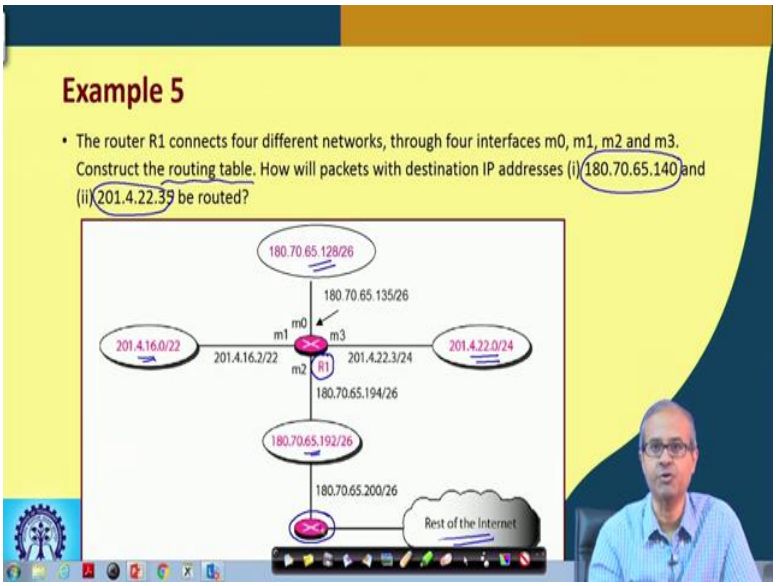


Now, let us look at the second example. Well this is also 135.46 or it will be one of the first two, but it is 52.2. Let us see what is 52.2. 52 is 00110100, this is 52. 2 is 0000 0010. And here again we will be taking this 22 bits, 8 and 8, 16 and we were taking 6 bits from here and these two bits are anyway 0, so if you do a bit by bit ANDing with this, it will become 01, this will be 00 anyway.

So, this will remain as 52, but you see, this is 56 and this is 60, so it is not matching with 52, so there will be no match, there will also be no match here, 190 also no match here. So, finally, it will go to the default, default in the routing table is mentioned as all 0s, this is the convention which is followed. All 0s as the address means it is the default route. And this flag G, you just recall, G indicates whether it is a direct route or an indirect route. If it is directly connected G, will be 0, if it has to be forwarded to another gateway then G is one. So, if it is default, you normally send the packet to the, you can say to the interface router or the border router who will be sending it to the outside world.

So, here through this interface the packet will be forwarded to this next hop and from there it will go to the right direction. The last example I leave as an exercise for you, this if you do a checking in a similar way, you will find that there will be a match with the fourth row. Third row there will be no match, but fourth row there will be a match right. So, like this you can actually check whether a given packet with a given destination address whether there is a match in the routing table or not.

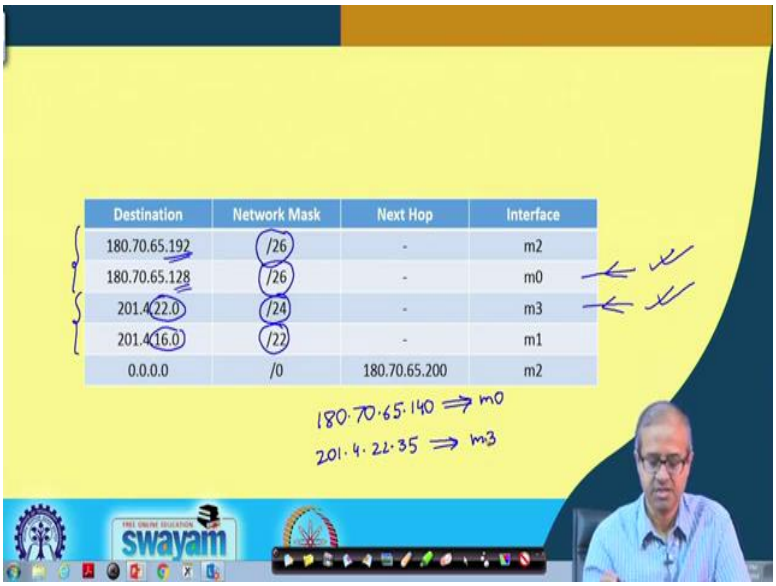
(Refer Slide Time: 28:10)



Let us take one last example. So, here we consider a router R1, this is our router R1. So, as you can see, there are four interfaces m0, m1, m2 and m3 and these are the networks which it is connected to, these are the network addresses and also in CIDR notation, number of bits of the network address is also mentioned 26, 22, 26 and here 24.

And through this, there is an external router which is connected to the external world, rest of the router ok. So, here there are two questions; one thing is that we are asking you to construct the routing table, and secondly, for these two packets, how they will get routed. Well routing table will be very simple, there will be four entries one corresponding to m0 with this network, m1 with this, m2 with this, m3 with this and default will be this, via this default it will go here.

(Refer Slide Time: 29:31)



So, I am actually showing you the solution, you can just verify, for the first network through m2 which is connected to m2.If you recall there are 26 bits of the address. So, it is slash 26 and this is the network address, through m0 also there is 26 bits like this m3, m1 and finally, m2 is the default which we will be sending it to the external router.

Now, you see one thing also I mean, I want to tell you with this example, you see this interfaces are not listed in order m0, m1, m2, m3, m4, they are listed in some arbitrary order apparently, first m2, then m0, then m3 then m1, but there is something orderly about this. You see we are talking about longest prefix match.Wherever there is a longest match, you take that as the match, others you ignore.

Now if we sort the network masks in ascending, in descending order largest one first. So, if there is a longer match, it will get matched first. So, you need not see the later entries, this saves the searching and matching time. If you sort your table with respect to network mask with the largest values first, then the first match you get that will be the longest prefix match, because that corresponds to the largest value of mask right.

Now talking about the IP addresses in the example that I mentioned; the first was 180.70.65.140, say 180; obviously, to be one of the first two. So, I again leave it as an exercise for you.You look at the first 26 bits of the address and see if you take the first 26 bits, whether it is matching with either this or this. Well in this case, if you see, you will

see that there will be a match with the second row for this packet. So, this packet will get forwarded over m0, but the other example was 201.4.22.35.

This again 201, it will be one of these two. So, first you look at the first 24 bits, check whether it is matching with 22.0. If not, you compare the first 22 bits, check whether it matches with 16.0 and then you decide whether there is a match or not. Now in this example the first one 24, there will be, there will be a match. So, there will be a match out only. So, this will be forwarded over m3 such way, in this way if I give you a networking scenario or a routing table, you will be able to calculate and decide that how the packets are getting forwarded. If I give you a destination address, you will be able to tell how the matching is taking place in the routing table and how the packets will get forwarded.

So, with this I come to the end of this lecture. Now here in this lecture and over the past few lectures I have talked about the routing techniques and we have also seen some examples of routing. Now all these routing techniques and methods will be very important for you in understanding later on how the actually network based attacks can be mounted or can be taken place.

Most of the attacks that we talk about, they are mounted through this IP via some routers. So, once a hacker gets hold of a router, if the routing table gets modified then packets can be routed arbitrarily as per the wish of the hacker ok. So, all these things we shall be seeing later.

Thank you.