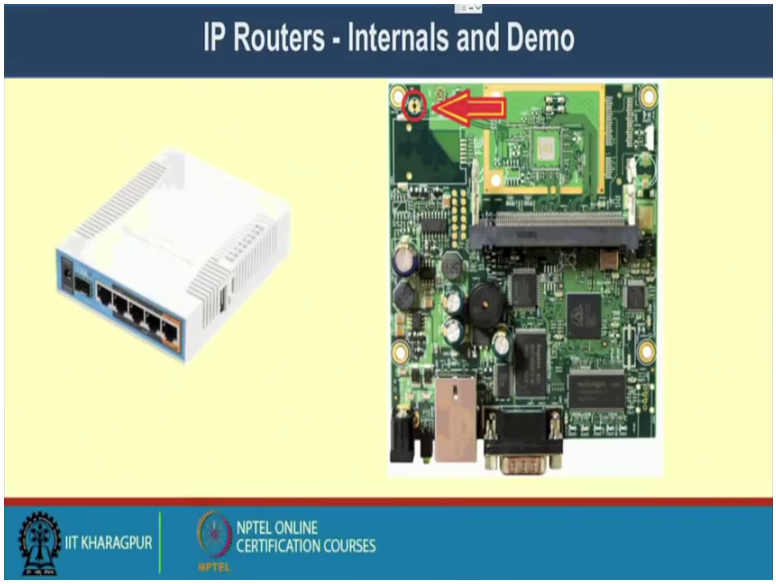
Computer Networks and Internet Protocol
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 42
IP Routers Demo

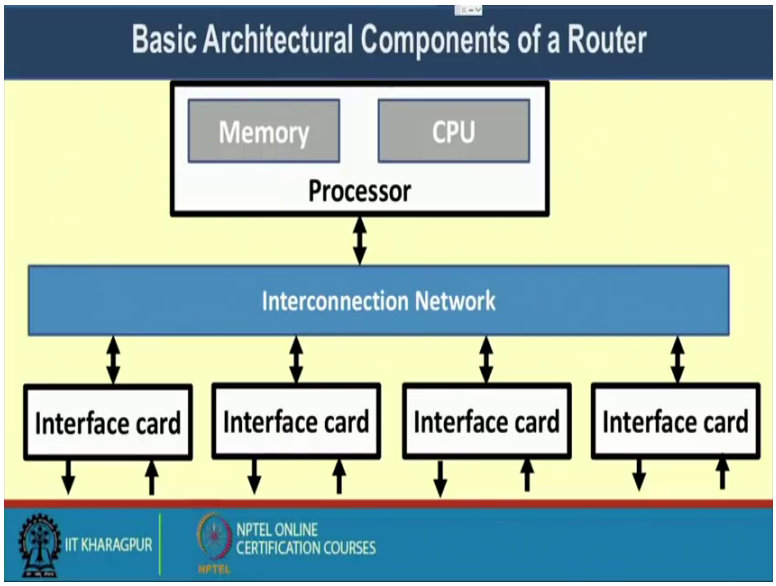
Welcome back to the course on Computer Network and the Internet Protocols.

(Refer Slide Time: 00:23)



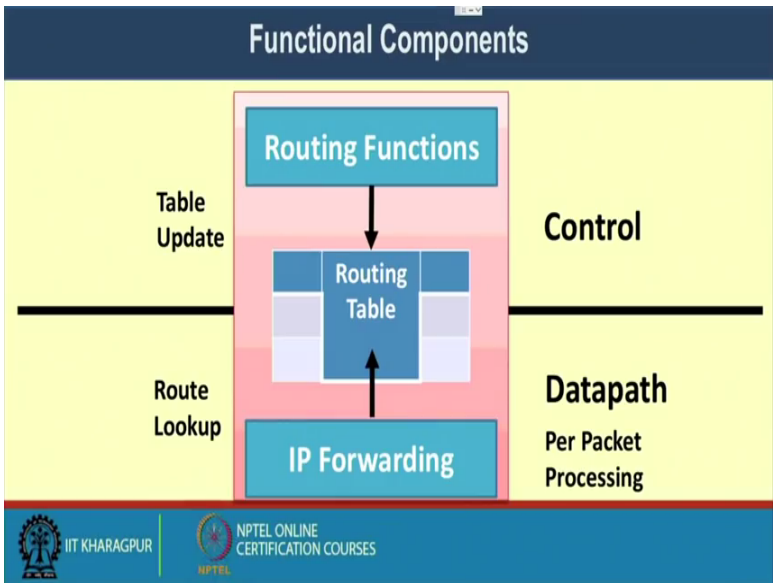
So, in the last class, we were discussing about IP routers, we have discussed about the different functionalities of the IP routers, and how a IP router look like.

(Refer Slide Time: 00:31)



So, specifically what we have seen that in a basic architectural components of a router, we have two different components. We have the route processor at the top and that route processor contains a memory and a CPU. And then we have a internal interconnection network bus with which the individual interface cards are connected and that interface card they work as the input-output for the routers.

(Refer Slide Time: 01:04)



So, in that continuation we have also seen that this entire router architecture is actually divided into two part, the control part and the data path part. In the control part, we have

different routing functionalities which are being implemented. So, in the later classes we will see different types of routing protocols which are used to populate the routing table, you will see that there are routing protocols like distance vector routing, link state routing, and in the internet scale you have a Border Gateway Protocol or BGP class of routings which are used to populate this intermediate routing table.

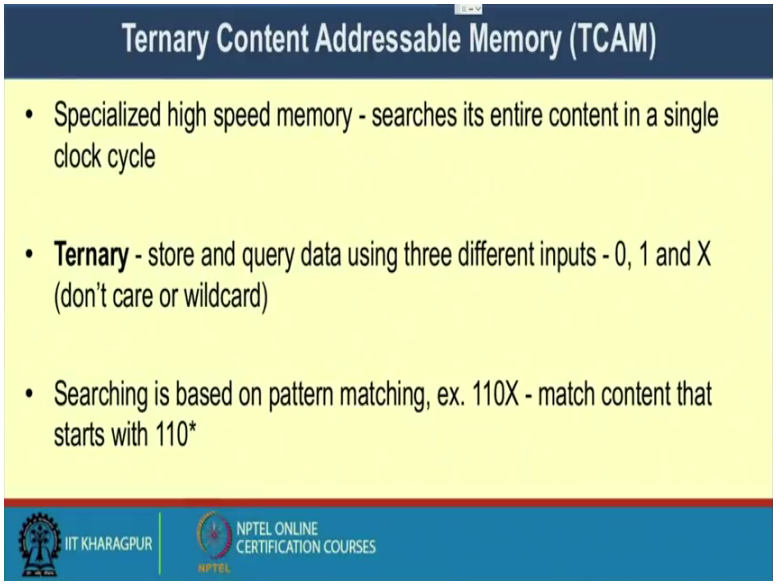
So, in the router control part we have these routing functions or the routing protocols which are implemented. And those routing functions or the routing protocol that we will look in subsequent lectures in details. They helps us in constructing the routing table. And then at the data path level, we do the per packet processing things. So, whenever you have certain input packets with that input packets, you look into the packet header; from the packet header you find out what is the destination IP address. Based on the destination IP address, you need to make a match with the routing table find out what should be your next stop and accordingly forward the packet to the next stop, so that was the basic architecture of the data path.

And we have briefly mentioned that this data path is need to be very fast, because at per second you have to possibly process some thousands or sometime a millions of packets if you are in a high speed network. And, that is why this data path is normally implemented in a hardware that we call as Ternary Content Addressable Memory or TCAM kind of memory architecture. So, in general in a typical router, in the control path or the control plane that is implemented as a part of the route software routing operating system which is a internet scale operating system, we have mentioned that there are different kind of internet operating system like a Cisco IOS. So, that particular software module implements your routing functionalities, your routing protocol, that software functionalities which need to be there to processor router and that construct the routing table which is there.

Now, we have seen that the data path need to be implemented in a faster hardware, we implement it in the TCAM type of memory architecture and the snapshot of this routing table is bring to the TCAM hardware in the form of Forwarding Information Base or FIB. So, that forwarding information base is basically looked up by the TCAM hardware to forward the packet to the outgoing interface.

So, we have the intermediate switch fabric that takes the input, make a match with the forwarding information base which is there in the TCAM hardware, and then it finds out what should be your destination interface along with the next stop. And that information is passed to the data link layer for doing further processing and the packet is put to the outgoing interface.

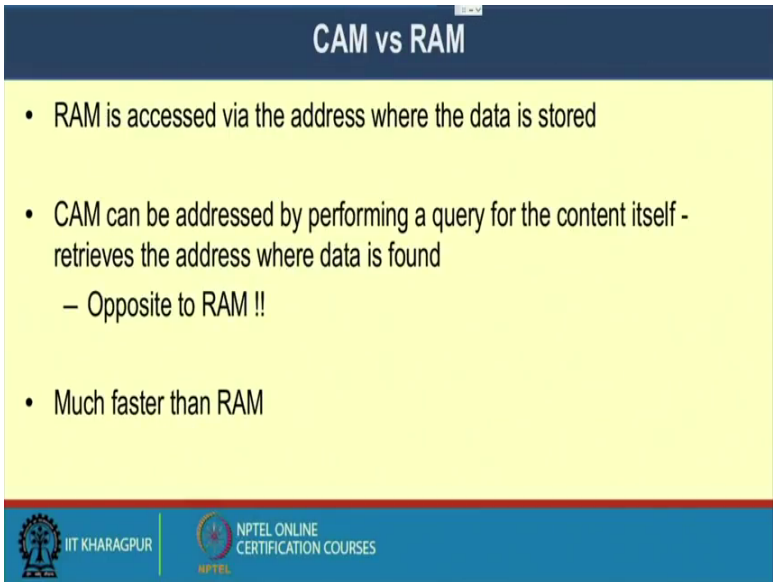
(Refer Slide Time: 04:27)



Now, we will briefly look into the architecture of this ternary content addressable memory or TCAM which is used to process your router. So, this TCAM is specifically a specialized high speed memory which searches its entire content in a single clock cycle. So, we call it ternary because it stores and query the data using three different inputs, either it can be the 0 or an 1 or something called the x. So, that is a don't care or wildcard condition. So, that is why we name it as ternary content addressable memory because everything is represent is either in 0, 1 or X that is the don't care or wild card condition.

Now, this searching in a ternary content addressable memory, it is based on pattern matching. So, one example is given here say for example, you want to find out 110x. So, you want to make a match with 1 followed by a match with 1, followed by a match with 0; and the fourth bit you do not consider. So, both 1101 and 1100 will get matched with this particular pattern.

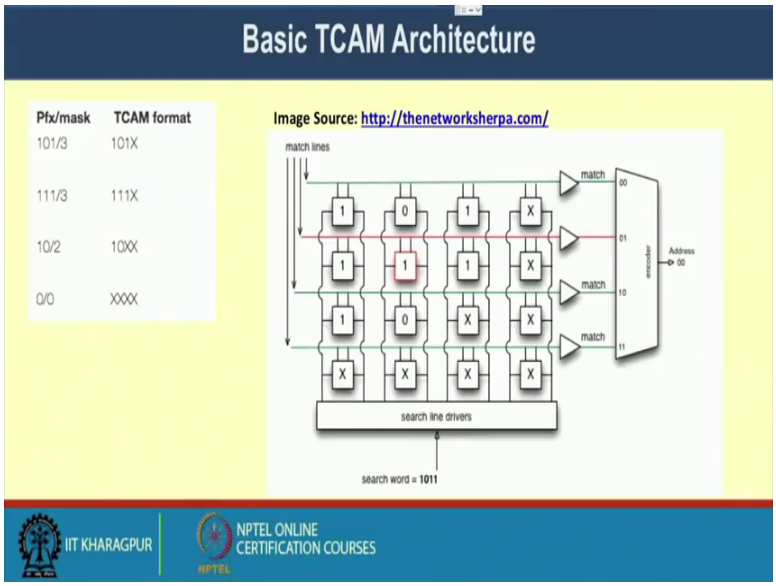
(Refer Slide Time: 05:35)



So, if we compare between this content addressable memory and our normal random access memory CAM and RAM, so this they are basically complimentary or they are kind of works in a inverse principle. So, RAM is accessed via the address where the data is stored. So, the operating system need to issue the address where the data is being stored inside the RAM. And then it sends that particular address and fetch the data from that particular address. So, RAM is basically accessible via this address; and it works in a kind of sequential address springs principle and at the same time at the random access principle. So, you can just pick up an address, go to that location, pick up the content from there.

On the other hand, CAM can be addressed by performing a query for the content itself. So, in case of CAM, CAM you do not require the address rather it restricts the address where the content is being found. So, here the search is based on the content itself not on the address. So, in case of a RAM, we provide the address and the output is the corresponding content at the data which is being stored at that address location. In the case of CAM, it is just a reverse like you are providing the content there you are searching the content there. If the content is found inside the CAM, then it will return back with the corresponding address, so that way it is much faster than RAM and that is why we use it for this network processing for implemented the forwarding information based inside a router data path.

(Refer Slide Time: 07:23)



So, here is a basic architecture of TCAM with an example. So, this right side diagram shows the different components of the TCAM hardware. So, we have different blocks that is the individual memory location, where the contents are being stored. So, here the in the top line the first block is storing as 1; the second block is storing as 0; the third block is 1; and the fourth block is don't care, so that is why because the fourth block is a don't care. So, you can have a match with either 0's or 1's.

Now, in a routing table, what we can do, we put the data in the format of prefix and mask that we have seen earlier. Now, for the simplicity we just put here an example of the prefix in a 3-bit format and the corresponding masks. So, we to say your prefix is 101, and the mask is 3; that means, if something is if your destination IP has the first 3-bits or the prefix has 101, then there will be a corresponding match. So, similarly we have a prefix of 111 with a mask 3, prefix of 10 with the mask 2, prefix of 0 with the mask 0.

Now, if you remember in the route matching principle, it is like that if there is a match in the first 3-bits that means, 101 and the remaining bits can be anything because this first 3-bits the prefix part it denotes your network IP and the remaining part denotes the host IP. So, during the routing procedure, we make a match with the network IP, so that is why we extract the network IP and make a match with that. So, in your 32-bit IP address format, you just need to look into the network address part, you do not need to look into the host address part for doing the routing.

The host address part is required to make the final forwarding at the last of router when it has received in the router where in the local area network where your machine is being located. So, in the last of router, you require the host address and in the previous case you just look into the network IP and based on the network IP you make look up. So, here your network IP contains the first 3 prefix bits. So, it is 101 followed by 3. Now, in the TCAM format, if you just for the simplicity assume that my routing address is not 32 bits my routing address is router address or the IP address is a 4-bit IP address well actual IP address is 32 bit, just for simplicity and for the explanation we are assuming that the address is for 4 bit address field.

Now, if 3-bit denotes the prefix then in the TCAM format it will be 101X. So, the last bit is the don't care condition and this last bit is actually you are denoting your host IP. Similarly for 111 and the mask tree in the TCAM format it will be 111 followed by X a don't care condition. For a prefix of 10 with mask 2, the first two bit will be 10 and the remaining two bits will be XX. When the prefix is 0 as well as the mask 0 this entire part belongs to the host part. We have a special meaning of this kind of addresses the TCAM format will be XXXX.

Now, whenever the things will get matched here in this TCAM format the things have been stored in this format here in the bottom, in the bottom most case we are storing XXXX, on top of that we are storing 10XX, then we are storing 1111 111X. And then finally, you are storing 101X, so that is my TCAM structure with these address format and address space.

Now, say we are we want to search a word of 1011 here. Now, how this search will be being done? So, we have this match lines this match line will trigger that which particular blocks need to be activated. So, if these four blocks are getting activated, during that time if you want a search word of 1011 that is a match with the last block XXXX, because all are don't care. So, whatever be the bits that will get accepted. Then we make a matching with the next block it is 10XX.

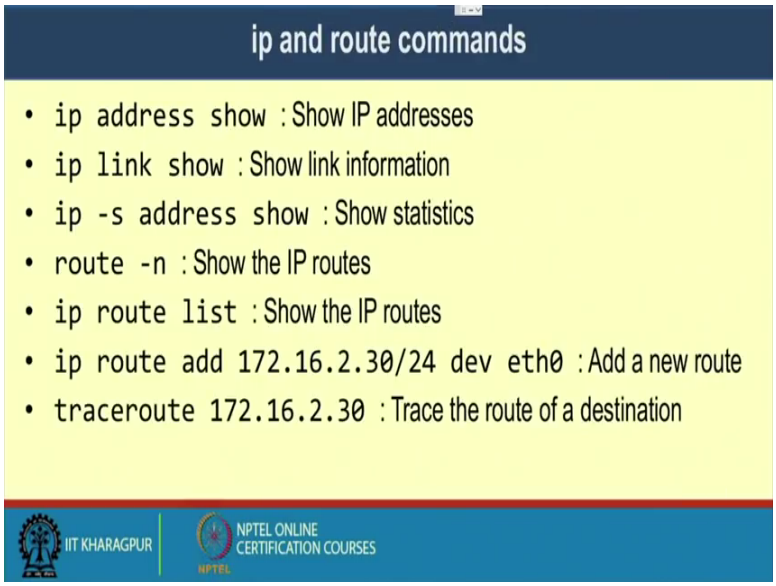
Again we have a match because we have first 10, this 10 will get matched here, then the two parts are XX. So, whatever we are providing here, here we are providing 11 that will see a match. The third one 111x that is not a match because, the second bit is 0, so here it is 1, so it is not a match. The fourth one is again a match. The fourth one is 1011, so 101

there is a match. And then last one is X - the don't care. So, there is a match there. So, we have a three match here. The first match is at address location say 00; the second match is address location 10; and the third match is at address location 11.

Now, we have an encoder that will return my final address. So, if you remember that in case of a routing whenever we do a routing match we take the longest prefix match. So, if there are multiple matches, then we take the final output as the 1, where there is the longest match. So, out of these four cases XX sorry the three cases where we have a match XXXX, 11, 10XX, and 101X. The longest prefix in the last 101X, because here I have a match with three different bits and I have only one don't care. So, the maximum match is here.

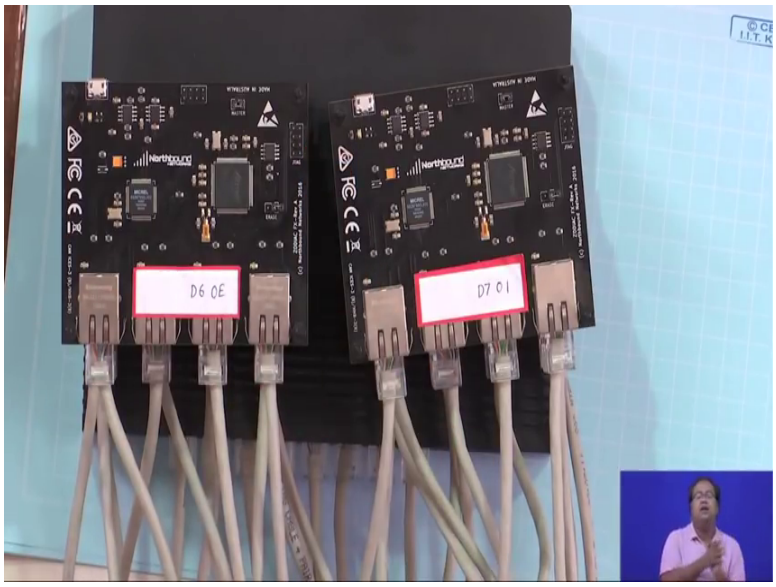
So, this encoder will return that particular address where you have the maximum match. So, the encoder circuit is to implement your longest prefix match principle to return back the final address, so that way you will get the final address as 00 indicating that the content is there. And in that particular address location the you whatever is there, whatever be the next information there that will be used to fetch the interface information, and the next stop information and there the packet will be forwarded. So, that is the idea of this TCAM hardware which makes the search based on the content itself and not based on the RAM based on the RAM architecture which makes the search based on the hardware. So, that is the idea of the TCAM.

(Refer Slide Time: 14:01)



Now, we will look into several IP and route commands. Before going to that, let me show you that how a typical router looks like. So, here I have a two routers, which are there and which are connected with particular switch So, you can look into this architecture.

(Refer Slide Time: 14:31)



So, this architecture, in this architecture what we have done here we have two router boot. So, this is one router boot, and this is the second router boot. And both of these router boots are connected to a layer two switch. So, this lower thing, this is a TP link switch which is a layer two switch. So, these two router hardware they are connected to the switch via the wire.

Now, a particular router looks like this indeed this is a small prototype of a router. The actual routers are even bigger than this one. So, here we have a four different chasses. So, you can see that this is one chasses; the second chasses; the third chesses and the fourth chesses. And every chesses has a four different interfaces. So, we have a 1, 2, 3 and 4 interfaces. And with these interfaces they are connected with these RJ 45 cable.

So, these RJ 45 cables are used to connect the wires with that router interface VT or machine interface. So, these are the input-output interface which are there with each of these input output interface we have these interface processor, and here I have this TCAM hardware and finally, the route processor. So, this is the route processor that contains the router software which is which need to be executed there and that router

software will help you to find out the routing protocol, run the routing protocol and do the stuff.

Indeed this particular router is a something called as software define networking router. In the next class onwards we will discuss about this concept of software define networking router. The idea of the software define networking router is that route control part the software part is not implemented or not kept inside the hardware rather you can connect an external controller machine with this router, where the routing control protocols will run. And that will actually generate the forwarding rules and those forwarding rules will be implemented inside the TCAM hardware that is there inside the router.

And then whenever some input packet is coming to one of these input interfaces, it will make a match with that TCAM hardware, and make the forwarding to the outgoing interface where it wants to forward. So, here we have all these different forwarding interfaces. So, among all these different forwarding interfaces, here we have four interfaces connected with every chasses. So, it is basically a 16 port router.

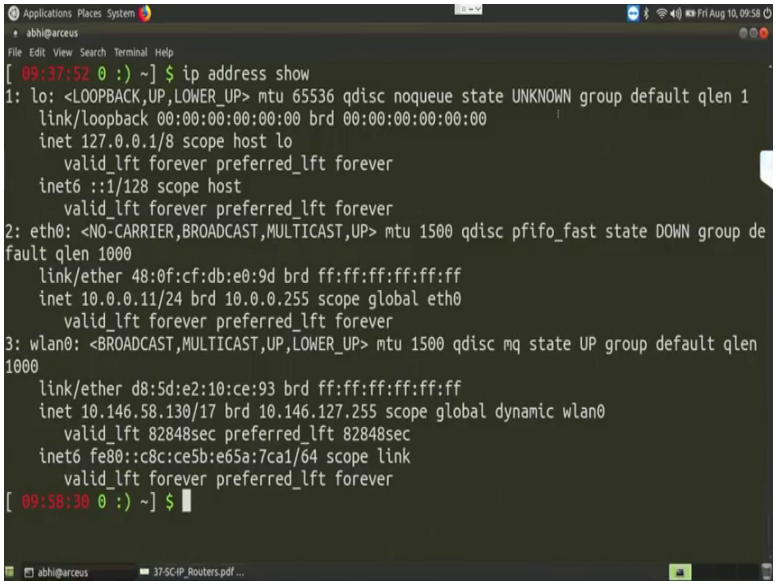
So, this one as it is a 16 port router. This one is another 16 port router. And both the 16 port routers are connected with this TP link switch, so which is a layer 2 switch. Now, normally what we do in case of our typical network architecture, we have this routers connected with the layer 2 switch and from the layer 2 switch again we are taking an output which is finally, connected to the machines the desktops that we have.

So, that way the packets come to the switch from the switch it comes to the router and then router takes the forwarding decision based on the routing protocol which is running inside. And after taking the forwarding decision, it sends the packet to the outgoing interface. So, this is the typical router which looks like this way. So, you have these routing boards which are connected into multiple chesses that we have briefly discussed in the last lecture. And finally, the input output interfaces through which the individual machines are being connected; so, this is the typical look of a router. So, these entire chasses we nicely put inside a box and amount it somewhere.

Now, let us come back to the slides where we were talking about different kind of IP and route commands to see different type of tools that you can use to look into the IP related

aspects of your machine, and at the same time the routing related aspects and configure your router. So, let us have a brief discussion about that.

(Refer Slide Time: 19:11)



So, the first command that we would like to see is something called IP address. So, show if you in a Linux based machine if you give the comment asIP address show. So, you can see that it will show you all the interfaces that you have in your machine. So, in this machine, I have three different interfaces; one logical interface which we call as the loop back interface. So, if you remember that earlier during the socket programming, we were specifying the host name as the local host, and that local host actually works on that loop back address. So, a loop back address, there the data is not going to some outside machine that means, it will work on the same machine.

So, on the same machine you have both the sender and the receiver. So, during that time, you can utilize that loop back loop back interface. So, this loop back interfaces just to look into whether the protocol stack of your machine is live or not; so, you can see that the loop back address as an IP address 127 dot 0 dot 9 dot 1 slash 8. So, that is the loop back IP address and the hardware address is all 0's. So, then there are other parameters.

So, you have this inet 127 dot 0 dot 0 dot 1 is the IP before address of the loop back interface and inet 6 is the ipv 6 address of that loop back interface. Then the next interface that I have is eth 0 that is the Ethernet interface the wag interface which is connected with this machine that has an link address. So, you can see that link slash ether

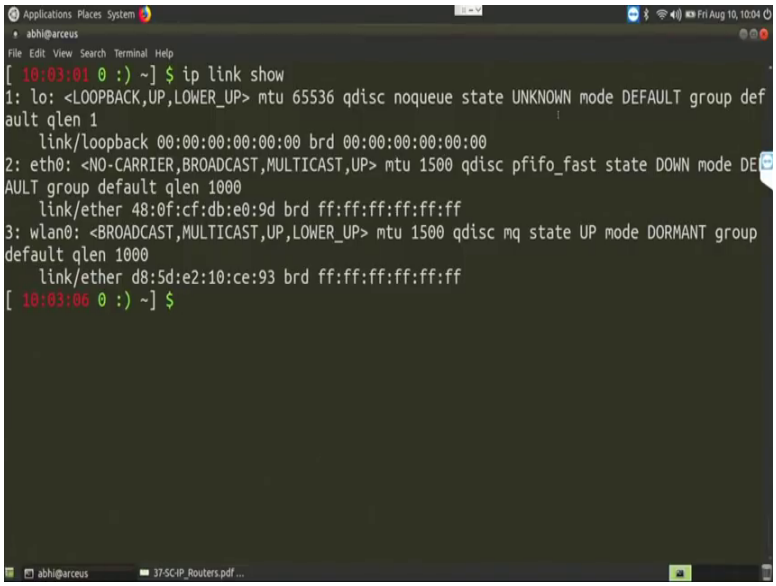
the hardware address or the MAC address is 48 colon 0 f colon cf colon db colon e 0 colon 9 d that is the hardware address and the broadcast hardware address or all fs, that means, all 1's. And the IP before address of these machine is 10 dot 0 dot 0 dot 11 slash 24 broadcast address is 10 dot 0 dot 0 dot 255, and this does not configure with the ipv 6 address on the ipv 4 address has been provided.

Now, coming to this WLAN interface; the wireless LAN interface which is connected with this machine. So, this wireless LAN interface has link or the ether address the hardware address as d 85 d e 210 ce 93, and broadcast address as all 1. Then it has a IP before address which is 10 dot 146 dot 58 dot 130 slash 17 that is the IP before address which is assign to this WLAN 0 interface the wireless interface; and the broadcast address as 10 dot 146 dot 127 dot 255. And it also has a ipv 6 address which is written in the next line inet 6, inet 6, fe 80.

So, this is the ipv 6 address for this machine, fe 80 colon colon colon colon. So, in ipv 6 discussion will discuss what does it mean. Then c 8 c colon c e 5 b colon c e 6 5 a colon 7 c a 1 slash 64 and that is the ipv 6 address of this. Now, all of this interface information you can also see that there is a parameter call mtu. So, if you look into the loop back case, in the loopback case, it is written as lo; then loop back up lower up then it is written as mtu 65536.

So, this mtu is the maximum transmission unit that means, the maximum number of bits that can be transmitted on that this particular interfaces in the form of a data packet. So, your data packets size your link layer packet size should not exceed more than 65536 for this loopback address, loopback interface. For the Ethernet interface, you can see it is written as Ethernet no carrier BROADCAST MULTICAST UP then mtu 1500, so that means, the mtu is 1500 bytes. So, you should not send more data than 1500 for a single packet in the Ethernet interface. Similarly, for the WLAN interface the mtu is1500. So, you should not send the more than 1500 bytes of data in the wireless interface as well. So, this is the individual interface information that we have.

(Refer Slide Time: 23:52)



Now, the next say command that we want to learn is ip link show. So, this command ip link show it will show the similar kind of information, but it will show the link layer property of the individual interfaces. So, it will show the individual link property. So, for the loopback interface, you can see that the link or it supports mtu of 65536. It uses qdisc, qdisc is a particular queuing protocol; then it does not have any queuing interfaces. It state is unknown current state, the mode the link mode then whether some group is defined or not then the qlen.

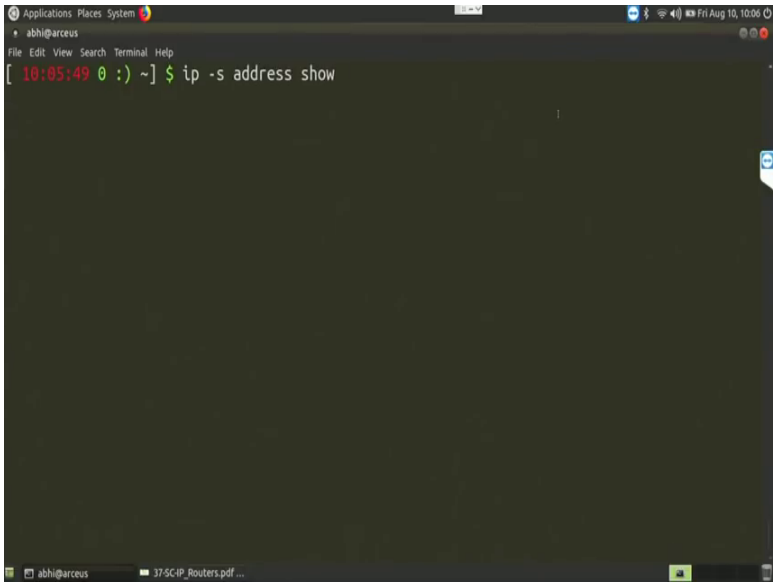
Then for the Ethernet interface, so actually in the loopback interface there is no such default q. So, your qlen is 1. So, whatever packet will come, it will immediately send that packet. So, there is no queue which is associated with this link. Now, in the Ethernet interface you can see that it has this individual support parameters followed by a mtu of 1500; it uses qdisc and it uses the q type of pfifo. So, this pfifo is the priority pfifo q it a first queuing state. It current state is down you have not connected any Ethernet interface with this machine. So, the state is down its mode is default group default and the qlen is 1000.

So, you can store 1000 packets of mtu 1500 bytes inside the q that it has. Similarly, for the WLAN, it supports BROADCAST MULTICAST, it is currently up. So, the mtu is 1500 bytes; the qdisc supports the q type is mq the something called a management q for the WLAN i triple E 82.11 network. So, this management q is actually a four layer q, it

four different quality of service classes its current state is up. We are currently connected to this wireless interface with this academic Wi-Fi router. So, this it is connected with these academic.

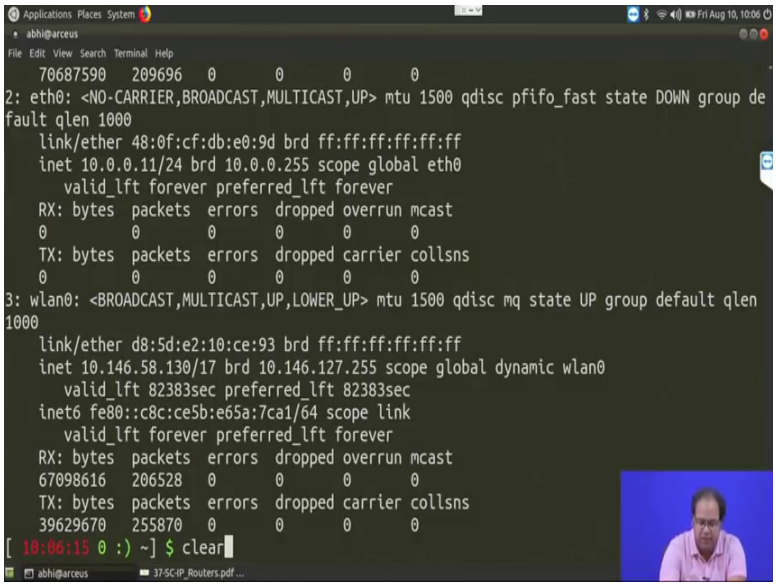
So, that is why currently it is up its mode is dormant, mode is dormant means the every packet that you are currently sending to this particular machine it will be send to this WLAN interface. The group is the default group. You have not defined any group and a qlen is 1000 packet. So, you keep 1000 packets of maximum mtu 1500 inside the management q that you have. So, this is about the link layer information that you can get from the comment.

(Refer Slide Time: 26:48)



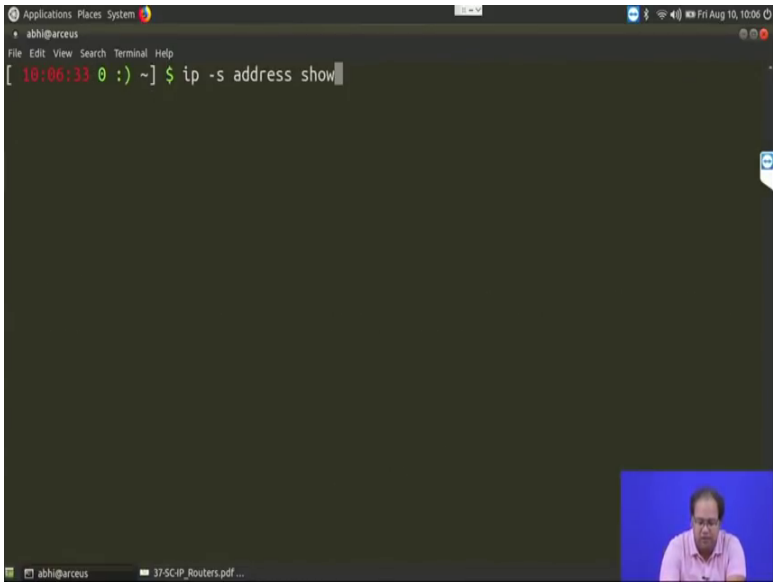
Then we will see some detail statistics of individual interfaces. So, for that we issue the command as ip minus s address show. So, earlier we have seen ip address show. Now, with that we are adding up this minus s option.

(Refer Slide Time: 27:07)



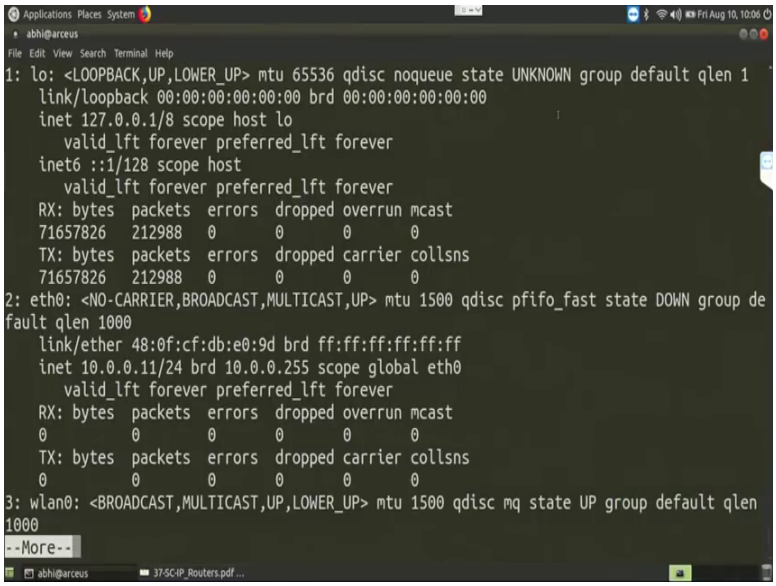
So, here you can see for the individual interfaces it gives the detail statistics. So, here the for the loopback interface, the statistics is given, then the Ethernet 0 interface. So, the loop back is not coming here.

(Refer Slide Time: 27:25)



Just so if I just because of the resolution if I make it more.

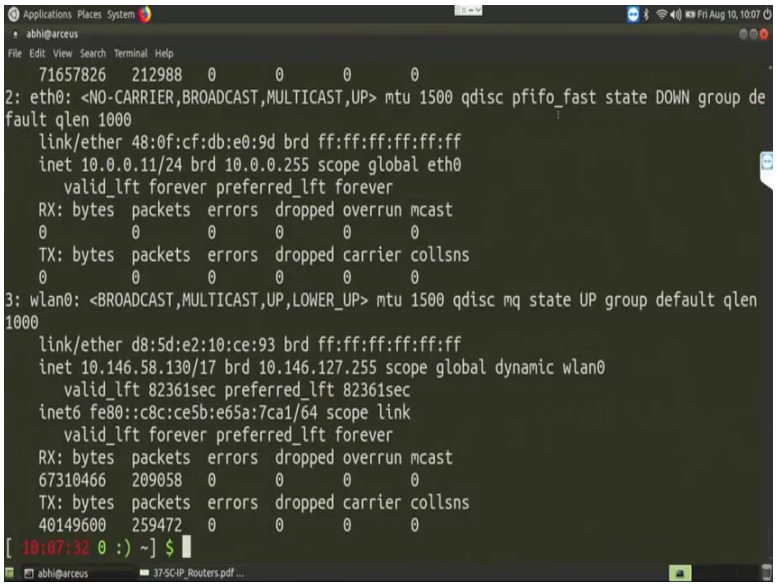
(Refer Slide Time: 27:30)



So, here you can see if initially the loop back information, the statistics for the loop back informations are coming. So, it says you about the total amount of received bytes total amount of received packets. So, whether some error has been occurred or not, how many packets are been drop, how many overrun packets, how many mutlicast packets.

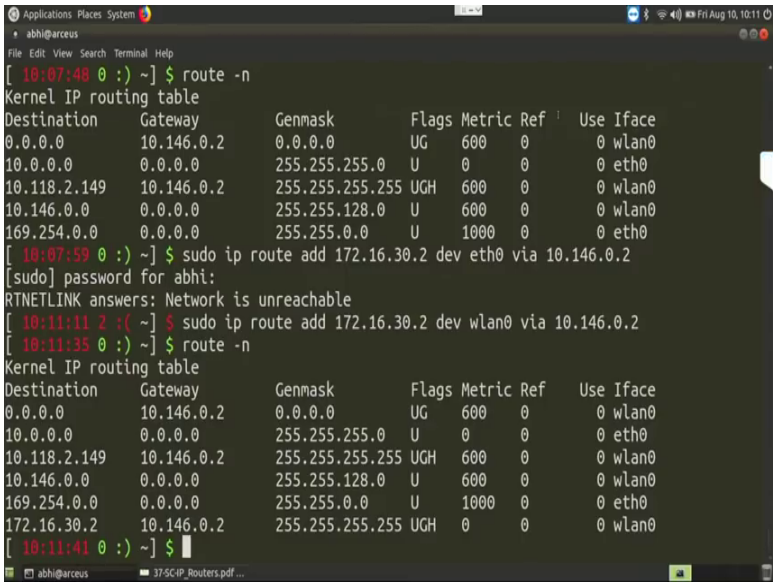
Similarly, for the transmit packets or it is the total amount of bytes that are been transmitted. Till now till the interface was life, then the total number of packets, similarly the error packets, the dropped packets, the carrier packets and the number of packets that has experienced the collision. Similarly, for the Ethernet interfaces, you have the Ethernet interfaces currently down we have not connected any Ethernet interface to this machine, so that is why it is coming to be the receive and the transmit bytes all are coming to be 0.

(Refer Slide Time: 28:24)



Now, for the WLAN you can see that it is having a amount of received bytes the amount of received packets from the time the WLAN interface became up. Similarly, the transmit bytes and the transmit packets, so that gives you a detail statistics about the link.

(Refer Slide Time: 28:40)



Now, we will see the route related things. So, let us make the command as route minus n. So, this route minus n will show you the routing table which is there in this machine. So, you can see that the routing table contain this parameters the destination IP followed by the gateway, the net mask, certain flag bit a metric of a individual paths, some reference

bits some use bits, and the finally, interface where this particular destination is connected.

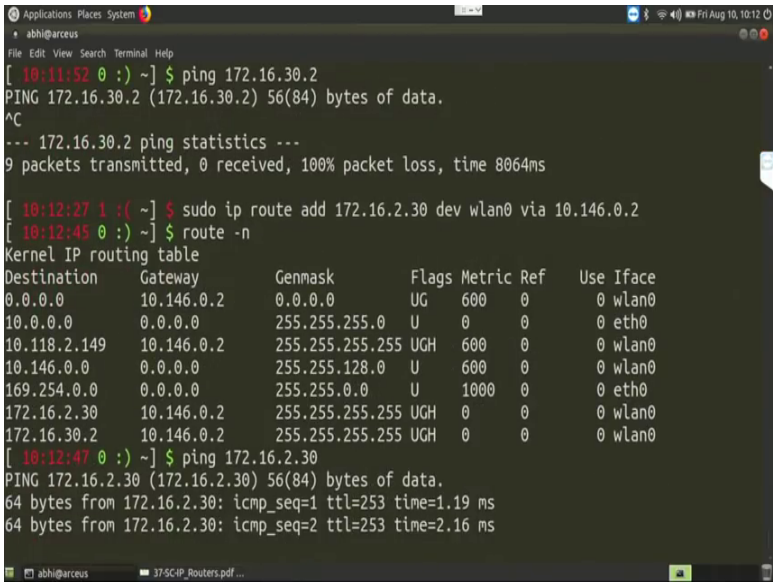
So, for example, if I will take say the destination IP as 10 dot 118 dot 2 dot 149 for that my default gateway is 10 dot 146 dot 0 dot 2 that is the next top ip. And for that net mask is 255 dot 255 dot 255 dot 255 then the default interface is wlan 0. So; that means, if you want to forward the packet to this particular IP, 10 dot 118 dot 2 dot 149 with a net mask of 255 dot 255 dot 255 dot 255, your interface will be wlan 0. You have to send it through wlan 0 interface, and your gateway will be 10 dot 146 dot 0 dot 2, so that means, my routing table.

Now, say if I want to add the new routing entry to this route table, for that you can use the command sudo ip route add, then you give the destination where you want to add up in the routing table, say I want to add 172 dot 16 dot 2 dot 30 dot 2 this particular ip. And say my interface is wlan 0 through which interface I want to connect it. So, dev eth 0, so this wlan 0 so, what we are trying to do here, we are trying to add the new ip route in this routing table.

So, my destination is 172 dot 16 dot 30 dot 2 this particular IP address I want to add. You can also provide the net mask in the form slash 24. If you are not providing the net mask that means it will take the entire path the 30 to be that is the net mask, based on your IP you can provide that net mask. So, the default interface is eth 0 and then I am providing the gateway the gateway address will be via. So, via say 10 dot 146 dot 0 dot 2. So, this will add a the routing table.

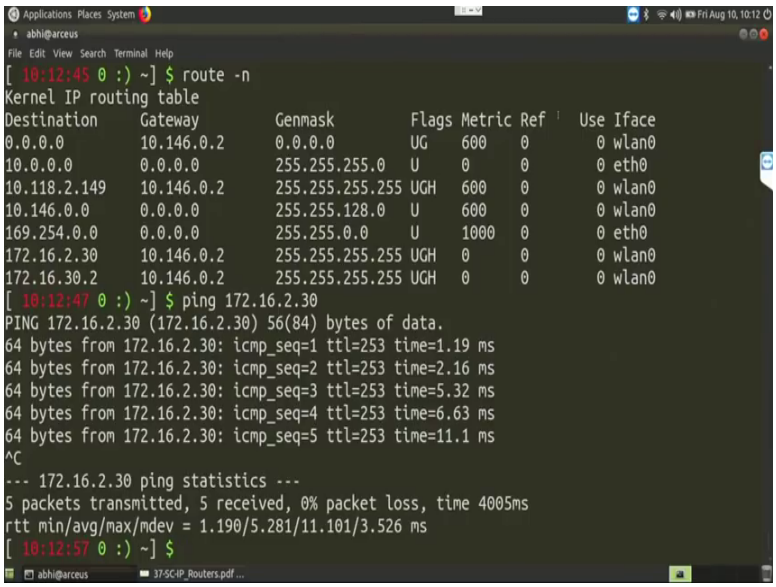
Now, to add the routing table you require route axis. So, it so, we have use this sudo command here it ask for the route password. So, let me give the route password. So, ok, so it says the network is unreachable ok. The network is unreachable message is coming because we are trying to add it the default interface at eth 0. Now, this eth 0 interface is down because this eth 0 interface is currently down. So, it does not get add up. So, let us now try to add it up in wlan interface. So, it gets added. So, now, if you make route minus n command, you can see this entry is getting added here 172 dot 16 dot 30 dot 2, the last thing. So, let me just clear it and make it again ok.

(Refer Slide Time: 32:42)



So, the last entry you can see in this routing table it is 172 dot 16 dot 30 dot 2 the gateway is 10 dot 146 dot 0 dot 2; the netmask we have not given. So, it has taken 255 dot 255 dot 255 dot 255 as the net mask and finally, the interface is wlan 0. Now, if you ping this machine, you can see, so the machine is not getting pinged, so that machine is not up. So, let us add.

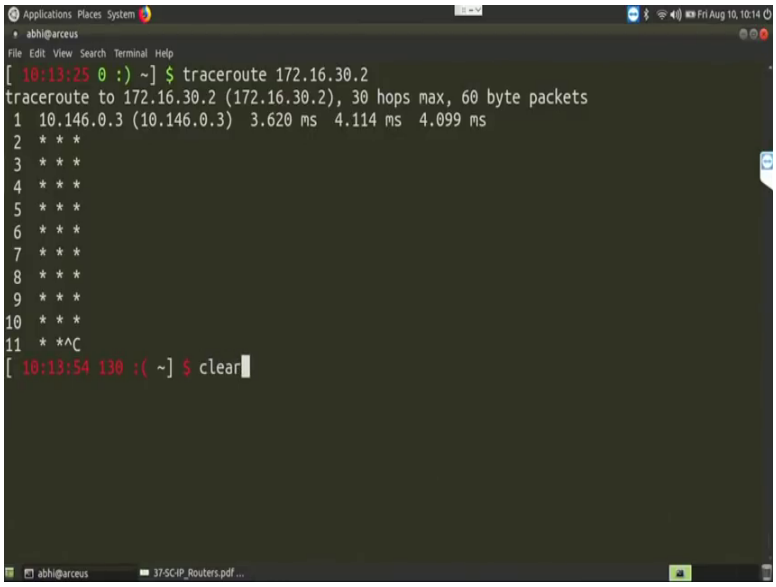
(Refer Slide Time: 33:49)



So, now we have added another IP 172 dot 16 dot 30 dot 2 a machine which is currently up; and the gateway I have given again as 10 dot 146 dot 0 dot 2 and a default net mask.

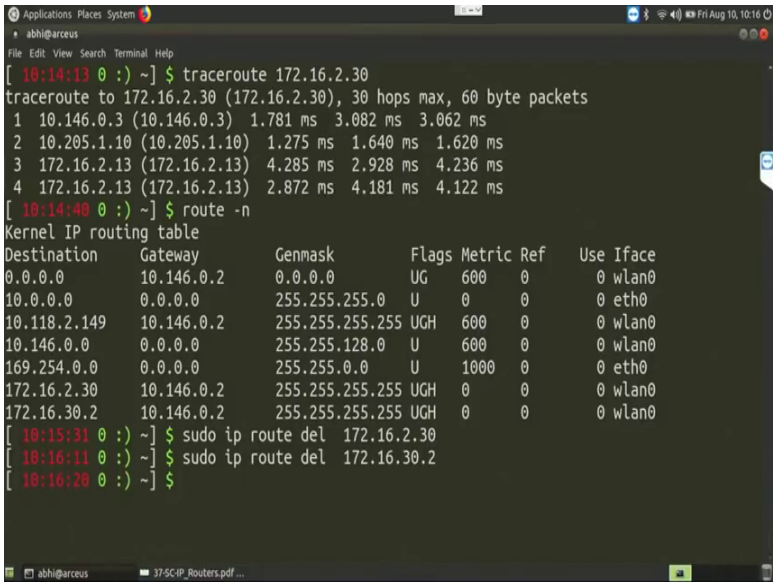
So, whenever I am pinging it is getting pinged. So, the machine is on and it is able to deliver the packet to that particular IP address. Now, you can actually see that which particular routing part it is following.

(Refer Slide Time: 34:18)



So, for that you can give the command as traceroute. So, if you make the command as traceroute as say let us try with both the IP addresses that we have added here 172 dot 16 dot 30 dot 2, so it will try to find out the path for that machine. So, what you can see from here, it has reached to the first top that we have added. So, in the first top it is 10 dot 146 dot 0 dot 3, the gateway address that we have given. After that gateway address it is not finding any path to forward that machine, so because this particular machine is currently down. So, the path is not there.

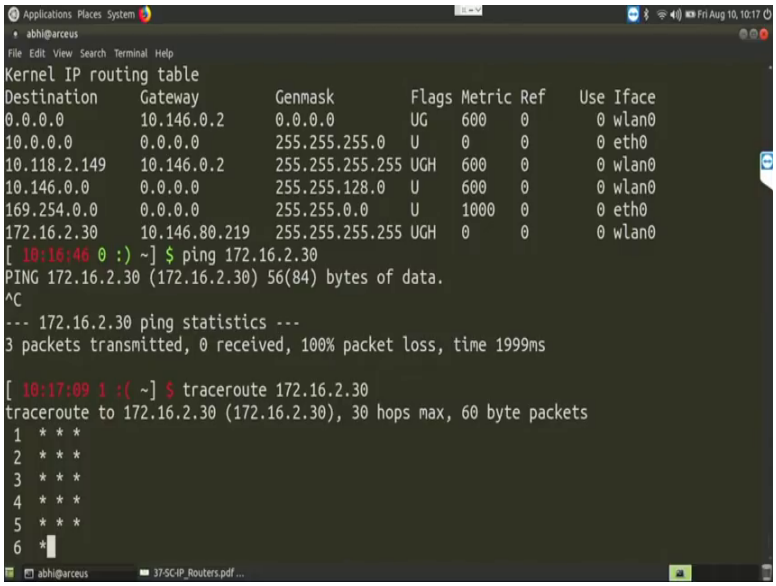
(Refer Slide Time: 35:05)



But on the other hand if you make a traceroute to 172 dot 16 dot 2 dot 30, so it will find out the path, it has found out the first top path. The first top path at 10 dot 146 dot 0 dot 3; the second top you can see is 10 dot 205 dot 1 dot 10; the third top as also came 172 dot 16 dot 2 dot 13 and finally, the four top is 172 dot 16 dot 2 dot 13. And here you can see that it show the response time that, what was the average response time to find out that individual hub.

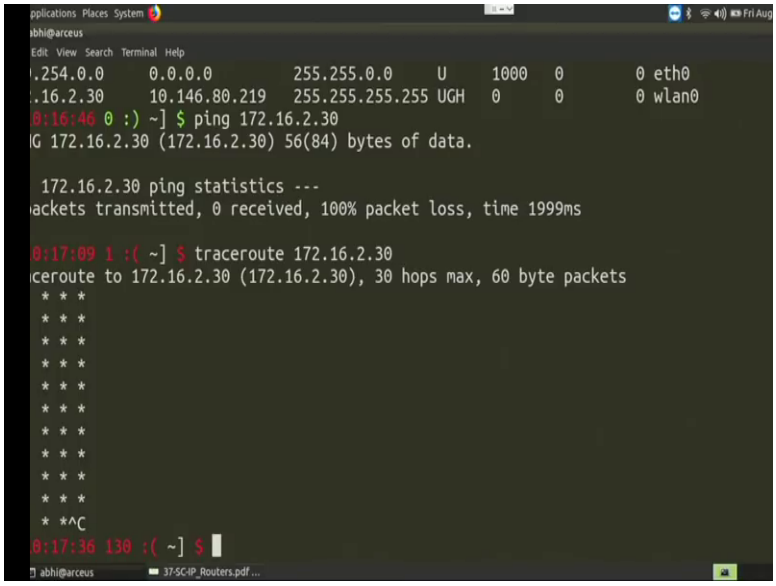
So, it has followed these particular tree hubs from this machine, it went to the gateway that you have specified 10 dot 146 dot 0 dot 3. Then it has went to 10 dot 205 dot 1 dot 10, then it has move to 172 dot 16 dot 2 dot 13. And that was the final hub from where it was able to reach 172 dot 16 dot 2 dot 13. Now, let us do one thing let us change the gateway. So, in the route minus n we had added 172 dot 16 dot 30 dot 2, my gateway was 10 dot 146 dot 0 dot 2. Now, let us delete this entry del and also delete the entry.

(Refer Slide Time: 37:15)



Now, instead of via 10 dot 146 dot 0 dot 2, let me put out some other address 10 dot 146 dot say 80 dot 219 ok. Now, you see that my last entry has changed from 172 dot 16 dot 2 dot 30 to 10 dot 146 dot 80 dot 219. Now, in this particular case if I try to ping this machine ping 172 dot 16 dot 2 dot 30, it will not pinging. So, if you make a traced out here, 2 dot 16 dot 2 dot 30. Let see what happens. So, now, you see it is not able to forward the packet, so all the hubs are coming as star star star star.

(Refer Slide Time: 38:28)



So, that is why whatever default gateway we are entering here, so it is using that default gateway to forward the packet to the final destination. So, that way you can actually so this entries produce the IP route that command which we are providing, they are the default routing entries. We call it as the static routing entry. So, we are including this static routing entries to dynamically configure or better to say statically configure the routing table and accordingly things are getting forwarded.

So, what I suggest you is to play with this kind of tools and see what you are getting while sending some packets or trying to ping some destination IP address So, hope this particular lecture gives you an idea about in a Linux base system, how you can play with different kind of a IP related tools and see different statistics from your machine. So, just try to explore that further.

Thank you all for attending this class.