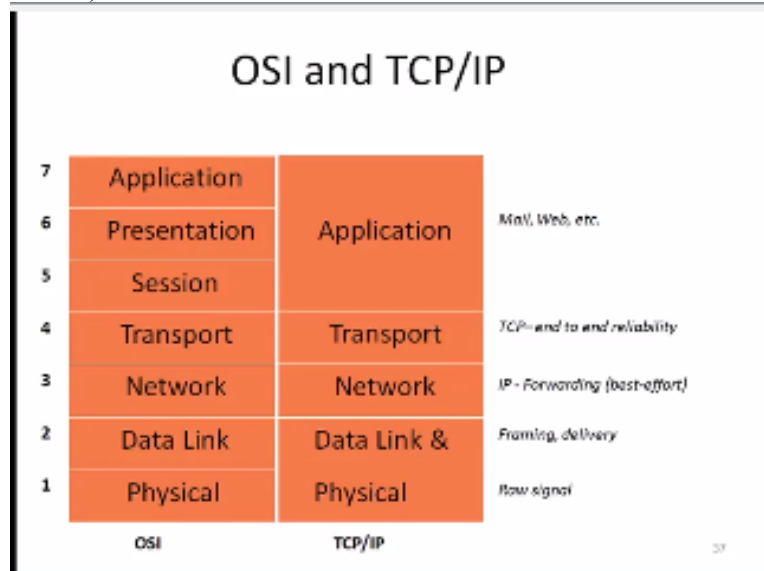


SEER AKADEMI

Linux Networking- Lecture-6

Hi everyone again welcome to this lecture today we will be continuing the Linux networking lecture before we begin actually let me recap what we did last the last lecture.
(Refer Slide Time: 00:21)



We actually started talking about the networking and we defined what the network is essentially the networking or how multiple computer or components they communicate with each other we started actually like I mean we then also collected our terminology these computer components they are all called nodes and we will be talking about nodes and then we also talked about the for moon characteristic of the network which is the size.

Which we measure as LAN, MAN etc topology like various types of stuff of the various way this configuration how they are all connected physically and then there is a physical characteristic also which is what kind of wiring used whether it is fiber channel whether it is copper we do it in terms of NBC or 150 kind of measurements and then finally the protocol essentially how they talk to each other.

Which is TCP is one of them good evening we are the one so we talk about this and then one of the concepts that we introduced during this lecture with open systems interconnection model or OSI which divides the whole networking into the seven layers form with varying degrees of complexity the application layer where you have complete visibility of the application. There you are launching the program you are thinning the program to a particular network and then once that program is when you decide to send and to hit the send button how they it is in transmitted that is what the OSI side use it like the various layers are the presentation layer the it

boosts the session layer and then it is the transport network data link and then the physical is there the actual computation happens to the wires.

And basically the bits are transmitted and we do not even call it bits it is basically the qualitative in fact a way of looking at OSI is from the bottom to the top which is the normal way that people always try to connected each because it is easier to understand that way so you talk about like how to picture transmitter and voltages then the data link layer which essentially forms the framing of the data.

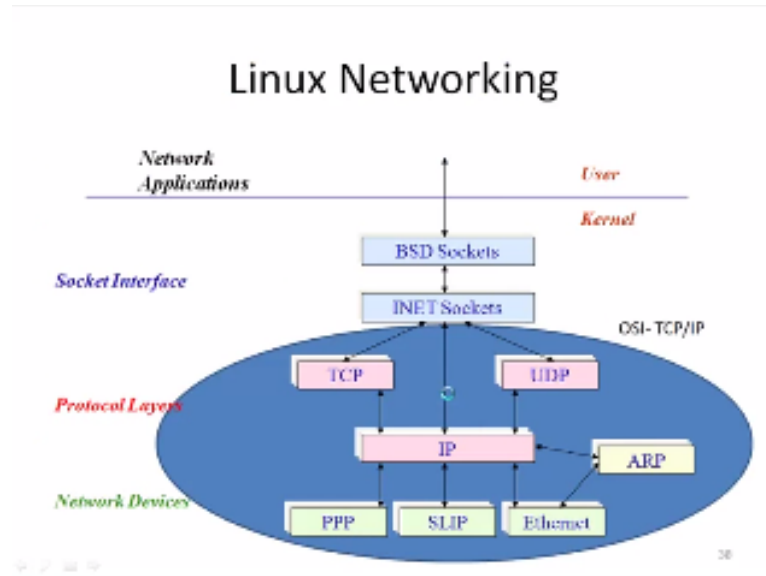
Then it goes into the network layer where basically has the IP covering also built in and then it goes into the transport layer which is born which offers the end-to-end offers into an reliability of the system and then the upper layers are the session here form and presentation and application there the data is aggregated more and then input of the application if you know the computer actually sees the complete picture or full data set.

All the getting is everything again it eliminated so example you also talked about how the OSI model differs from TCP/IP and the TCP does the top three layers as combining one and then essentially the all the upper-level applications mail web extra data sent in the application layer and then progressively like I mean you add bits basically break up the data and then you put how you broke up.

On those kind of road maps in to this so broken up pieces and then send as piecemeal into the various layers below and then the layers below them they can communicate we also saw like the 16 or essentially like five words sorry six 32-bit words which constitutes the IP header which is used by the IP layer sensitive and that is network layer to forward the messages and then we also saw like I mean how the various points before essentially.

Like our post is different from a router and how far higher the chain that the message has traveled before it is distinguished and then it is copied to the appropriate destination so we saw some of those.

(Refer Slide Time: 05:22)



Examples I also wanted to put this picture here which kind of summarizes all our discussions or so forth as you know again in the Ethernet layers of lowermost layers which then this is a link layer essentially which goes into the network layer visit the IP layer and then you have the transport layer the TCP layer so these are all buried under the bottom of the chain whereas the eternal actually like all these things with all these correspond to the Eternals side. And then the user just sees the top level and we also saw an example of a client-server architecture where the client opens up some communication channel it actually opens up something called a socket then when it so essentially like the server creates a socket it binds an address to the socket and then it basically waits at the point whenever the client wants to communicate client also creates a socket and these sockets are matching. So they see you in connect and once it sends that message to that appropriate socket and the server has a socket each sensor sends back another message to accept that socket at that point the connection is made and then the packets are send one by one into the server and then so services and then it sends back those packets as well so the send and receive goes hand in hand this simple client-server model is used in many applications. One of the key things that we learnt was also the HTTP how we open up a web site or essentially they can we make a server service request how that gets into the server and then how the server services that occurs so in the data centers you will find this for a lot impact one of the structures of the datacenter is that basically they also divided into layers there is a specific HTTP service layer and then followed by an application layer and followed by database layer. Which all of them work hand-in-hand to provide the best service possible or the user so that is the big introduction.

(Refer Slide Time: 08:14)



Today I am not going to ask you to do any exercises or activity we will all we will combine a lot of with activities into one movie lap all for this session today the main topic is going to be the IP addressing this is one of the topics I think is important from a general understanding perspective mainly because as VLSI designers you will be in situations where you have to make sure that how to debug a network.

And probably you may have to also correct some of the issues that are in the network and all of them like by remotely logging in and then also even do some little bit of system administrated again as I mentioned earlier this entire course is not to make you a system administrator this still focuses on the usage of the systems so we will only be doing that but I still wanted to give you like a little bit of basics on IP addressing.

So that you are well prepared like I mean if somebody says that hey this is your network address or this makeup is not working more disturb net is not working something like that then you know what they mean and how you can give them that information so did that introduction let us go into the IP everything so the first question that we ask is what is the purpose of IP address.

(Refer Slide Time: 10:13)

Purpose of an IP address

- Unique Identification of
 - Source
Sometimes used for security or policy-based filtering of data
 - Destination
So the networks know where to send the data
- Network Independent Format
 - IP over anything

40

Why do we need the IP address so IP address is unique identification of the source so sometimes like you can use it for security and policy based filtering of data what this means is you can avoid certain or you can bounce back certain sources of their from where the service requests to coordinating the other one is when it originates from a low level server or a high level based on that you can set priority.

And we can set the voltage data needs to be taken in and which data needs to be revisited and then the IP address also provide a way to uniquely identify a destination so that the networks know where to send the data to so you need to have an IP address to receive the data while as a receiver of data you will be checking the IP address or whichever the message that is coming.

So in fact the network administrator's use the idea within very effective way this way they try to block certain network they identify the networks based on their IP address so that they can put it in the block table so that even if you try to IP address they can block it typical examples as you would move like porn sites and things like that basically there you cannot get into electronic public computer or just little or even like world computer.

The reason is the IT department knows the IP addresses of formal systems and then effectively block from any message is going to go from the office usually this is and network independent format that is what you need so that it is not tied to a given Network and one of the reasons why internet became popular is also because of this teacher is not tied to in network any particular type of network. So it is basically IP can be over so this is another key thing to remember so, what does it do action.

(Refer Slide Time: 12:52)

Purpose of an IP Address

- Identifies a machine's connection to a network
- Physically moving a machine from one network to another requires changing the IP address
- TCP/IP uses unique 32-bit addresses

-

So look at that so the IP address identifies a machine connection to a network so whenever a network receives a message it knows essentially later in which machine actually originated the purpose there are no likes curious request so coming to the network which can destabilize that move when you move from machine to machine even like I mean physically moving a particular machine from one network to another network you it requires a change of that the addresses.

So in fact this has become an issue because say like I mean now you actually change providers of Internet service and then suddenly new provider comes in and then you have to now you IP address there this is all different and then everything else is different that is okay but then you buy a new computer or the new changes router in your home system you do not want everything to be fiction.

So there are ways to actually also control this form there is like dynamic IP allocation that is what most of the international do because they know that the service is to just one mode but inside that node if you change anything they do not really want to know be there as long as they can uniquely identify that it is you who is originating mortgages they are affected with it so this dynamic IP addressing actually have become pretty popular.

So up to your point it may be a static one but then inside that we can make it into that and then TCP/IP use this unique 32-bit address and let us look at how they use this 32-bit address in the next slide.

(Refer Slide Time: 15:10)

Basic Structure of an IP Address

◆ 32 bit number (4 octet number):
(e.g. 133.27.162.125)

◆ Decimal Representation:

133	27	162	125
-----	----	-----	-----

◆ Binary Representation:

10000101	00011011	10100010	01111101
----------	----------	----------	----------

◆ Hexadecimal Representation:

85	1B	A2	7D
----	----	----	----

42

So it is a 32-bit number divided as for active number so it is 8 bits so the representation will be like and say 130. 3.27 162. 125 that is one IP address so that is the decimal representation in binary you can also like represent this into the following here you can say basically that it is 100010101 so that represents this one and 133 it is a single number and then 27 is represented as the 11011 and then 162 is a game 10010 then same for 12520111110 and sometimes this is also represented in exodus move.

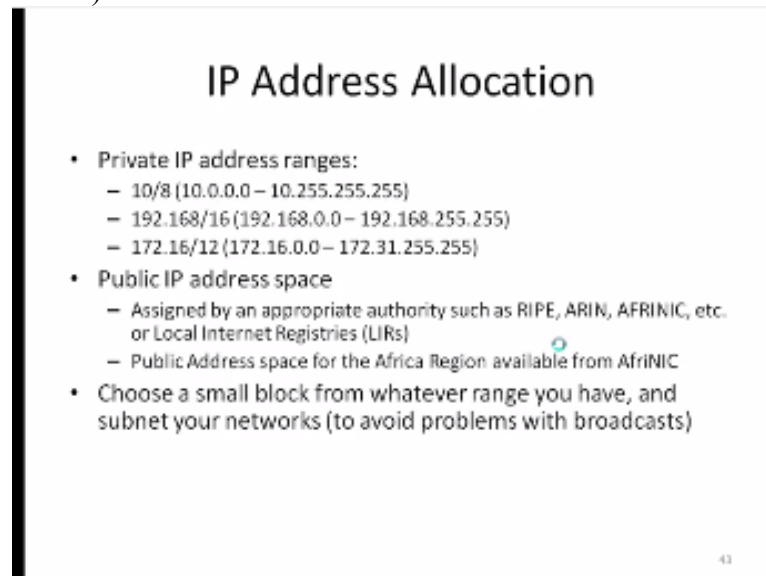
For example the same number can be like 85 1B A2 7D in Linux systems typically like I mean people represent their IPs is a symbol or they all out the IP addresses in hexadecimal in fact there are some commands which we will talk about in the later part of this lecture the commands to get data from the coming of machines and see like I mean how they are accepted so we will talk about that later.

So now let us look at how this IPS officer allocated as I already mentioned the there is a static IP address which is what was very prevalent and until they ran out of the address space and then they start doing with dynamic and then dynamic also used to solve certain issue or the providers do not want to know like I mean how many computers are connected to the network I mean they want to know like I mean number what they do not really care.

Which ones are connected today in a typical home you can find up to like maybe ten devices connecting into the internet in various forms sometimes I mean they are all like connect it together you know very easily again you can found your TV is the TV is are connected your all your mobile phones on the computers are connected printers are connected I do not know maybe even like your alarm clock.

Whichever want one you can think of they can easily be connected to the network or your network storage is another big thing right now so that is another attached story so now if you add up all these things 10,15 easily if you pause that number and so the key question is how do you provide the unique addresses to all of them so let us look at how that is done how the IP addresses are allocated.

(Refer Slide Time: 18:37)



IP Address Allocation

- Private IP address ranges:
 - 10/8 (10.0.0.0 – 10.255.255.255)
 - 192.168/16 (192.168.0.0 – 192.168.255.255)
 - 172.16/12 (172.16.0.0 – 172.31.255.255)
- Public IP address space
 - Assigned by an appropriate authority such as RIPE, ARIN, AFRINIC, etc. or Local Internet Registries (LIRs)
 - Public Address space for the Africa Region available from AfrinIC
- Choose a small block from whatever range you have, and subnet your networks (to avoid problems with broadcasts)

43

So here actually like them in there can be like two different IP address structures only is the private IP address they range from 10 to 8 essentially like every 10 or 8 and then like 10.000 10.0.0.0 to 10.255.255.255 which is a maximum an IP number and also like I mean the other one is 192 and 168 192.168 or 16 that is another set of private IP addresses and then 172.16 and that is another one to.

So here it is listed here basically like the 192.168.0.0 through all the way and then this 172.16 that is again goes to one side the 172.31.255 so this IP address ranges within two you know can you can look at your machines inside the network they will all have like this IP address been like more than 192 and 172 but the public address space is mostly like minutes there are many authorities assigning these members.

Some of these authorities of this right here in AFRINIC etc or there are local internet registry also known as LIRS in United States there are several companies allocate this address right now like I mean even like new companies started allocating different address so essentially let you provider actually like has taken a block of address from one of these authorities and then they start allocating it to their customers as well as.

So essentially like I mean the bottom line is you have a small block from whatever range that you have and you subnet your networks so essentially and think of the larger Internet as a hierarchical element there you may just get like one address would not be limited from one address you create a subnet which has more of them so and then you pay the subnet it and then you take that avoided So once you have this thing like I mean you would not have to broadcast at this wide range.

(Refer Slide Time: 21:52)

Addressing in Internetworks

- The problem we have
 - More than one physical network
 - Different Locations
 - Larger number of computers
- Need structure in IP addresses
 - network part identifies which network in the internetwork (e.g. the Internet)
 - host part identifies host on that network

44

So now let us look at how do we addressing the internet works so the problem that we face is essentially like anymore we have or than one physical network because there are all the subjects and they are in different locations large number of computers so we need a structure in the IP addresses so to define the structure we need to have one portion which defines the network or the network part this defines.

Which identifies which network in the internet work that this belongs to which is basically the Internet and then the second part of the as this is the host that identifies the host on that network so every network has an address that is what this the first part is and then the second part is okay in this network where does this host taken.

(Refer Slide Time: 23:03)

Address Structure Revisited

- Hierarchical Division in IP Address:
 - Network Part (Prefix)
 - describes which physical network
 - Host Part (Host Address)
 - describes which host on that network

I_p

205 . 154 . 8	1
11001101 10011010 00001000	00000001
Network	Host

- Boundary can be anywhere
 - very often NOT at a multiple of 8 bits

45

So now we talked about the 32 bit now this how do we divide this into hierarchical IP address hierarchical division so the network part defines the physical network that it belongs to and then the host is identified which is the whole that is connected to bottom so here like I mean the part that in go previous slide there are these four numbers the objects basically the first three octets now determine the network.

And then the last one determines what the host is, so essentially like I mean even though we talked about this the boundary can be really anywhere may not be like even a multiple of eight bits because so you run out of the address space or the original ones we can actually like allocate more to the host if there are more hosts.

(Refer Slide Time: 24:12)

Network Masks

- Network Masks help define which bits are used to describe the Network Part and which for hosts
- Different Representations:
 - decimal dot notation: 255.255.224.0
 - binary: 11111111 11111111 11100000 00000000
 - hexadecimal: 0xFFFFE000
 - number of network bits: /19
- Binary AND of 32 bit IP address with 32 bit netmask yields network part of address

46

And that how we determine what is the network part and what is the host part if they is by using a network mask so let is look at what the network mask is the network mask help define which bits are used to describe the network part and which are used all the host so there are different representations again for the network mask you can define the network mask as just a decimal dot notation which is 255. 255. 224. 0 this is one of the examples.

So here you can see that actually like the network is up to here that is the first 816 the 21 sorry 19 bits and then the remaining all the zeros are the host part so the 19 bits first 19 bits will represent the network and then the remaining ones in this 13 bits represent the post address binary form that is what shown here and then the hexadecimal focus if you can describe the mask which is FFFFE000.

So typically like I mean your network mean once it assigns a once you become a part of the network host or whatever given machine parts becomes a part of the network the network will assign a mask essentially based on how many computers in the network are in the network based on that designs so mask and then the way that we generate the IP addresses is just a simple binary and of the 32 bit IP address if the 32 bit net mask.

And then we get the network part of the address so here a simple binary and will provide the first 19 bits which is essentially the network and then remaining on the host so you can use this simple add function to actually separate out the network and Ip address and host and allocation or verification.

(Refer Slide Time: 27:11)

Classless Addressing

- IP address with the subnet mask defines the range of addresses in the block
 - E.g 10.1.1.32/28 (subnet mask 255.255.255.240) defines the range 10.1.1.32 to 10.1.1.47
 - 10.1.1.32 is the network address
 - 10.1.1.47 is the broadcast address
 - 10.1.1.33 ->46 assignable addresses

47

Let us look at the classless addressing IP address with the subnet mask defines the range of address in the block essentially so you so once you have these subnet masks essentially like an

range 1.1.32 or 28 that defines the range from 10.1.1.10 to 32 to 10.1.1..47 with the above subnet mask so here the 10.1.1.1.32 is the network address and then the 47 becomes the broadcast address.

And then the 33 to 46 the range in between and they can be assigned to other hosts or as some other space actually this we can be assigned as a network addressing network addresses that you can open.

(Refer Slide Time: 28:26)

Forwarding

- Computers can only send packets directly to other computers on their subnet
- If the destination computer is not on the same subnet, packets are sent via a "gateway"
- defaultrouter option in /etc/rc.conf sets the default gateway for this system.
- IP forwarding on a FreeBSD box
 - turned on with the gateway_enable option in /etc/rc.conf otherwise the box will not forward packets from one interface to another.

48

So now let us look at how the computers forward the packets based on these addresses so then the packets are receive the computers can only send packets directly to other computers only if they are on the subnet if the destination is not part of the subnet which is identified by the network address then they are sent to Gateway the Gateway is kind of you can think of central router and that actually sends it to the other networks.

So gateway is something that communicates between the two networks and then within the network the packets can be sent directly and then the default router option in /etc/ RC .conf on upon text the default gateway person system so the one thing that you can find out you can do a less on this file to see where is your default gateway and what or what and what is the mission this is and then basically like them in IP forwarding on a free BSD box.

This is turned on with the Gateway enable option in the etc of the other one otherwise the box will not power the packets from one interface so let us look at the DNS itself.

(Refer Slide Time: 30:15)

How DNS (Domain Name System) fits

- Computers use IP Addresses but Humans find names easier to remember
- DNS provides a mapping of IP Addresses to names and vice versa
- Computers may be moved between networks, in which case their IP address will change BUT their names can remain the same

So DNS is what is the domain name system where the computers use the IP addresses but the again like I mean or humans it is very hard to remember those IP address so DNS provides a reverse mapping of the IP addresses to the machine means and why source have been actually like those core things so this is something that basically we can look into and then we can see like what domain name of a particular IP or if you have a domain name then you can also compare to sometimes so this is the one this is one of the lists there the computers are moved between the networks.

The IP addresses will change but the domain names are the names of the remain the thing so like I mean before like Casper or whatever the name of the machine so that always remains the same in whichever network that goes into so the way that we keep it that way is to use a domain name system file.

So the DNS file if you look at it that we have the name listed and we can easily see that I mean what is important and this particular computer this particular machine So let us look at some of the useful commands that we can use to navigate the network.

(Refer Slide Time: 32:05)

Network Troubleshooting Tools

- Ping
 - Send ICMP ECHO_REQUEST to network hosts
- Netstat
 - Print network connections routing tables, interface stats etc.
- Ifconfig
 - Configure network interfaces
- Traceroute
 - Print the route packets take to network host
- Tcpdump
 - Dump traffic on a network

53

Here I am actually talking about the commands again the comments actually follow the same higher same syntax that we all have out there all are familiar with by now it is which is a command named followed by a demon followed by oh sorry domain name followed the option followed by gone so the first command is ping command ping is used to send this ICMP echo request to the network course.

So essentially it is actually command by itself basically it instructs the receiving computer to send an echo of the ping basically so for example if you want to see that the network is a particular machine is alive or dead you can use a ping then you use the ping command to you know you send a ping command to that machine so that if the machine receives that ping man then it sends you back a message saying that a attitude.

So then you know that actually efficiency if it is not this can go on pinging for a while and then you know that either the network is having an undue delay or if that machine is it that you are trying to reach is so dead so typically we do this before we send more and if IP request steady basically like last lecture which is the file transfer protocol or transferring files between systems and so doing that actually we will be studying in more detail in the next section.

As to how we can teach can be done and what are the different configurations for FTP but the bottom line is in order to the thing is used as a prelude to doing an FTP this so that I mean you can see the resolution like then you can send this net stat is another command this prints out the network connections routing tables the interface that etcetera we know that all these things are these terminologies in reading both previous lecture.

The routing tables are the tables they are the machine knows okay house IP is the mapping and bottle closes instances and so how to quickly reach the destination essentially like I mean if it

receives the packet from this particular computer or this particular IP address to what should be the next IP address those kind of that kind of information is in the working table the network connections again it prints out the nearest neighbors.

Who are all connected and how they are connected and also like the in today is tasks like what kind of ports are open there which ports can be used for communication things like that if config is a command that is used for configuration of networks , so in ifconfig actually you can configure the network into issue there are good examples if you do a man or despotie you should be able to get a lot of good information ago to this one.

Trace route is as a command to print the route that packets are taking to the network course so as you know like the Internet itself is a big aggregation of the network hardware of all connected together by ways we saw the Gateway example machines. so the tracking the route that some packet is taking some packet is following it may be like very difficult so here essentially like I mean this uses the IP protocol time-to-live field one of the protocol.

That we talked about IP address itself and then it from there it attempts to see like the response from each of the Gateway along the path so that it understands what the path it takes to reach the destination so here essentially the mandatory parameter is the destination post name or the IP address the IP number all the other ones basically if it you do not have to specify and a simple default and give you either.

Here the usually the it also sends out a probe Datagram we know like what the data gram is since it is where we specified in both IP layer and below that Datagram is typically occupies data basically but even like I mean if it is more than content with increase or by specifying an opening so again I will ask if this do a man of a trace it off to get like more information regarding the particular command.

So usually if it gives you like I mean bunch of hosts it gives you the various it gives us a DNS table listen to me before it gives you the host name and its IP address and then it also gives you like I mean what time it is sticking like I mean how many hops for it each one is stable.

And then what are the what is the time that it is taking each of the whole system you so some of the LSS based commands use these commands to follow certain things and to understand certain and functions essentially then the last command that we will talk about is the TCP dump TCP dumps the traffic on a network again this, it the TCP dump actually brings out the headers of the packets on the network interface that match the Boolean expression.

So you can also like to give this Boolean expression again this goes through like I mean that same the options followed by the argument here essentially like I mean specified options and

then it turns out that, so TCP dump may not be a command that you can actually run it unless you have a permission ball or system administrator permission but you can still type `man TCP dump` and see like I mean what it is means.

You should generate whole bunch of information essentially so and there are various nodes that you by which you can dump information so if you want to print all the packets arriving at a destination you can give the TCP dump on that particular host and then you can also say like I mean okay you want some preferential packets only like show certain things or you can also say like okay this I want to see whether what is the traffic between two hosts.

So again these are the comments that are mainly by the system administrators to troubleshoot lot of these issues I just wanted to give you a favor of how they do it and then what kind of thing goes on underneath I hope this is useful for you again I think the piece this is pretty much the end of today is lecture we will be picking up from this point in the next one in to summarize today we mainly talked about the IP addressing.

Talked about how the IP addresses are formed why the IP address is not needed the 32 bit IP address there is also the address of the IP or the address of your computer which essentially constitutes two pieces of information one piece of information is the subnet where it belongs to as I sort of submit and then the second piece is each so on post ID inside that subnet and even though this is represented as 4,8 bit numbers or four octal numbers.

In reality the network address would be some bits of information and then host ID can give different set of bits they all need to act to the 32 bit but inside there is a bit how partition is up to you and so typically like that is determined by it is for the subnet mask that we talked about for the network most essentially like the by just looking at the network mark you can figure out how many bits are the addresses.

How many bits are the part of the network address and how many bits are part of post at this so this I hope this is useful and then the also open commands towards the end as so all the system administrators use these tools effectively to manage the system again I just wanted to just remember if you remember one command and that is the ping command bit.

Which is using many more times all the other commands are very sharing based by us in our feed again thanks a lot thanks for listening we will pick it up from beginner from this point and in the next lecture thanks once again.