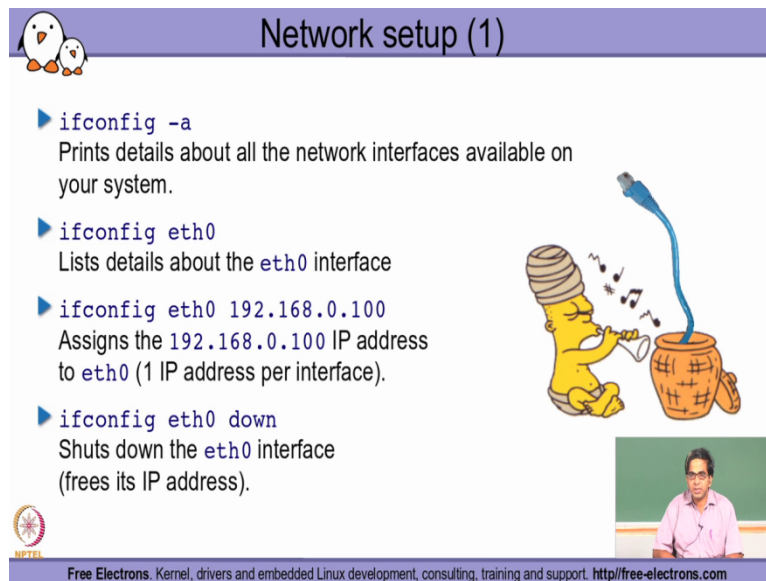


**Information Security**  
**Sri Vasam V S Principal Consultant**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**  
**Module 25**  
**Linux File Comparison**

So in this module we will be basically looking at some of the simple commands that we need to run to configure our Linux system for enabling the networking part of it.

(Refer Slide Time: 00:30)



**Network setup (1)**

- ▶ `ifconfig -a`  
Prints details about all the network interfaces available on your system.
- ▶ `ifconfig eth0`  
Lists details about the `eth0` interface
- ▶ `ifconfig eth0 192.168.0.100`  
Assigns the `192.168.0.100` IP address to `eth0` (1 IP address per interface).
- ▶ `ifconfig eth0 down`  
Shuts down the `eth0` interface (frees its IP address).

Free Electrons. Kernel, drivers and embedded Linux development, consulting, training and support. <http://free-electrons.com>

So a system could really have multiple Ethernet port which is available. So those Ethernet ports could be on the board or it could be connected as a add on card. Now for any kind of port whether it is networking port on the board or connected as an add on card are there has to be a configuration that has to be done and this configuration is typically on a per port basis

So for every port we need to basically set the IP address we need to configure the default gateway we also need to specify the Subnet Mask and then finally bring the interface up. So what is referred to as port is sort of abstracted out as an interface from the Linux world and you will find that all the kind of networking configuration command always refer to something called as an interface but these interface is nothing but what we refer to a port in the physical form.

So the command `ifconfig` stands for interface config is the command that is very commonly used for doing the complete network configuration as far as a Linux system is concerned. So

the `ifconfig` command if we basically use the `minus a` option the `a` here stands for all. So if use the `minus a` option it basically prints out all the details about the network interfaces that is available on the system. So when we say interface is available on the system it essentially means what the different interfaces that I have been detected at the Hardware level by the OS when it was booted up and also subsequently right?

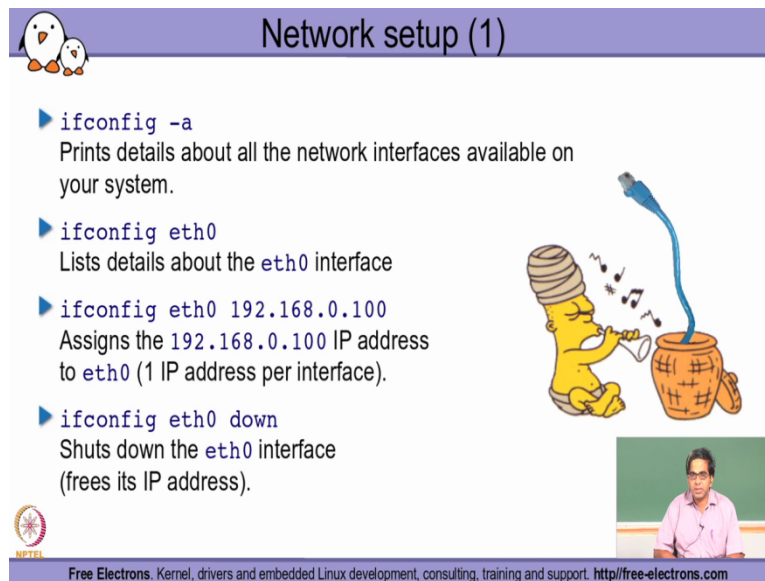
So when you use the `minus a` option if you for example have two Ethernet ports available on your system that is basically the RJ45 ports and let us say that your system is also having the Wi-Fi capability you will typically see three interfaces listed here apart from what is called as a loop back interface. So there is an interface name called as `lo` that is typically standing for loop back, so this is the interface that will be used by my IP stack to do a looping back of the data whatever has actually being sent down by the higher layers backup into the same higher layer.

So any kind of data that is actually being sent to the loop back interface will never get out of the system but it will be looped back into the system to the higher layers of my stack hour so that will be used by my data whatever there any kind of data never get out of the system but it will be back into the system.

So depending on how many interfaces I have on my system the physical interfaces that I have on my system the output of the `ifconfig minus a` will vary. if I want to specifically list down the details about any one interface alone so I would say `ifconfig` the name of the interface the typically the default name of my first Ethernet interface is `eth0` and if I have a second Ethernet interface the default name for that is `eth 1`.

So if we actually say `ifconfig eth 0` it will give me the details only about the `eth 0` interface. So the details that `ifconfig` command will typically print is what is the address ip address that has been assigned on the interface whether it is actually right now up or not how many bytes that this interfaces are sent out, how many it has actually received. So every detail about that interface so what is the Mac address of the interface and so on and so forth will be typically printed out by the `ifconfig` command.

(Refer Slide Time: 04:20)



### Network setup (1)

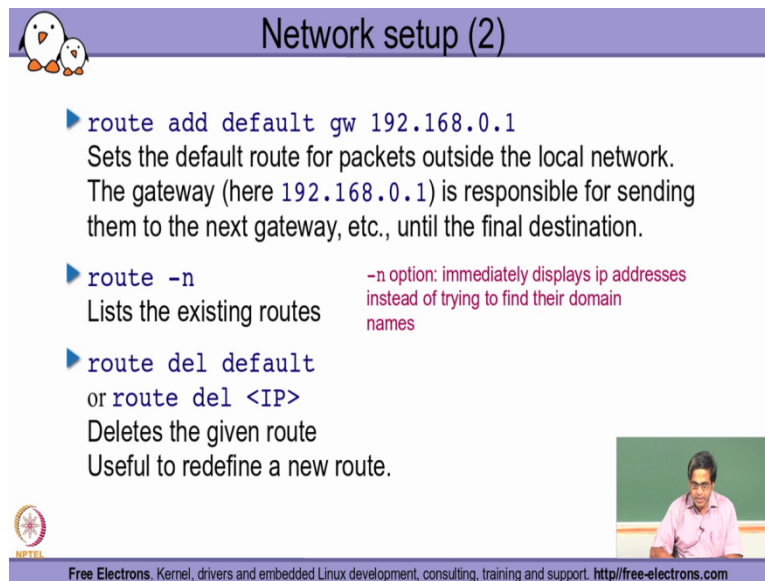
- ▶ `ifconfig -a`  
Prints details about all the network interfaces available on your system.
- ▶ `ifconfig eth0`  
Lists details about the `eth0` interface
- ▶ `ifconfig eth0 192.168.0.100`  
Assigns the `192.168.0.100` IP address to `eth0` (1 IP address per interface).
- ▶ `ifconfig eth0 down`  
Shuts down the `eth0` interface (frees its IP address).

Free Electrons. Kernel, drivers and embedded Linux development, consulting, training and support. <http://free-electrons.com>

Now if I want to specifically assign IP address to an interface I would typically use `ifconfig` command by `ifconfig` the name of the interface so if I want to basically assign IP address to `eth 0` so `ifconfig eth 0` followed by the IP address. So `192.168.0.100` so this will essentially assign the mentioned IP address to this particular interface and after which when the interface is brought up any packet in the network that has actually been assigned to the destination address marked as `192.168.0.100` will be received by this particular interface or this particular system.

So this is basically how I would go ahead and assign the IP address for a interface, Now if I want to bring down the corresponding interface I say `ifconfig eth 0 down`. So apart from the IP address here I could also specify the net mask as an additional argument I say net mask and then say whatever is the net mask that I want to set it to then I basically also give the gateway. So what we mean by the gateway here is that every packet that is actually originating out of the system through this particular interface should be having a particular gateway IP address configured so that the packets out of the system will be sent into that particular gateway IP address whatever has actually being configured.

(Refer Slide Time: 05:49)



### Network setup (2)

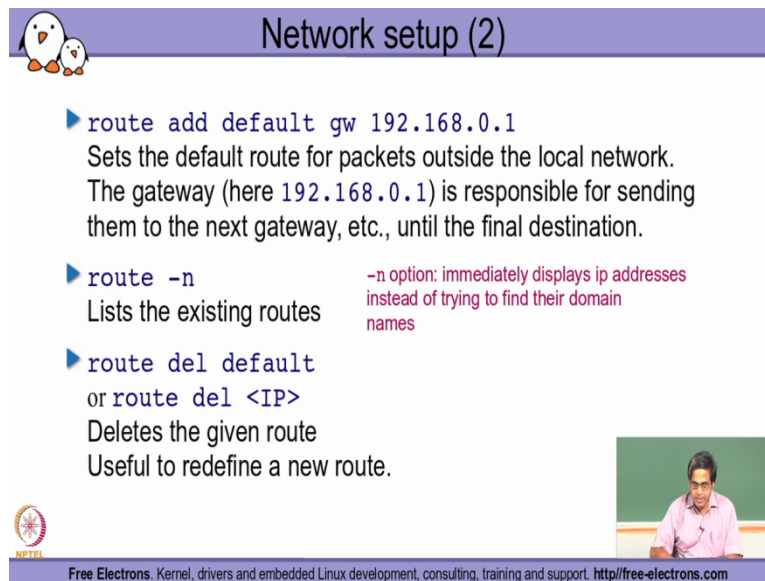
- ▶ `route add default gw 192.168.0.1`  
Sets the default route for packets outside the local network. The gateway (here 192.168.0.1) is responsible for sending them to the next gateway, etc., until the final destination.
- ▶ `route -n`  
Lists the existing routes  
*-n option: immediately displays ip addresses instead of trying to find their domain names*
- ▶ `route del default`  
or `route del <IP>`  
Deletes the given route  
Useful to redefine a new route.

Free Electrons. Kernel, drivers and embedded Linux development, consulting, training and support. <http://free-electrons.com>

So how do I add this gateway so I have the route command for it so we basically say route , then we say what operation we want to do so here we want to add so what do we want to add we want to add a default gateway, so what is the IP address of the default gateway? So then we finally specify the gateway IP address, so 192.168.0.1 is the IP address of the default gateway in this particular system, now what exactly is the default gateway any packets any network packets that is actually originating out of the system so if you are for example running a browser so you specify the URL as part of the browser URL field saying http colon back slash www.yahoo.com right?

Now the browser is going to generate an http packet this packet is actually going to go down all the way in my down into the IP layer and when it comes into IP layer it basically conflicts the IP data gram packet and then this packet when it comes down should basically be knowing, where this packet should be sent to from my system right? So this is a laptop on which I am originating a traffic the packet the network IP packet should basically know from this particular system where should it be sent to right? So that next hop that is basically what we called technically is what we configure here as a default gateway.

(Refer Slide Time: 07:18)



### Network setup (2)

- ▶ `route add default gw 192.168.0.1`  
Sets the default route for packets outside the local network. The gateway (here 192.168.0.1) is responsible for sending them to the next gateway, etc., until the final destination.
- ▶ `route -n`  
Lists the existing routes  
*-n option: immediately displays ip addresses instead of trying to find their domain names*
- ▶ `route del default`  
or `route del <IP>`  
Deletes the given route  
Useful to redefine a new route.

Free Electrons. Kernel, drivers and embedded Linux development, consulting, training and support. <http://free-electrons.com>

So all packets that are originating on this system in which this particular route command is being run will have the packets sent to this particular IP address that is getting configured as a default gateway through this command called route right? So I say route I want to basically do the add operation. So what do I want to add I want to add the default gateway now what is the IP address of this default gateway I specify that IP address as a next argument in my command line ok.

Now the next option that we very commonly use with the route command is a minus n option so I could either use the minus n option to basically list down the existing route or I also have an alternate command called the net stat. So if I use the net stat minus nr option that command also in the system will be printing out the current configured routes on my system in which I am running the command, right?

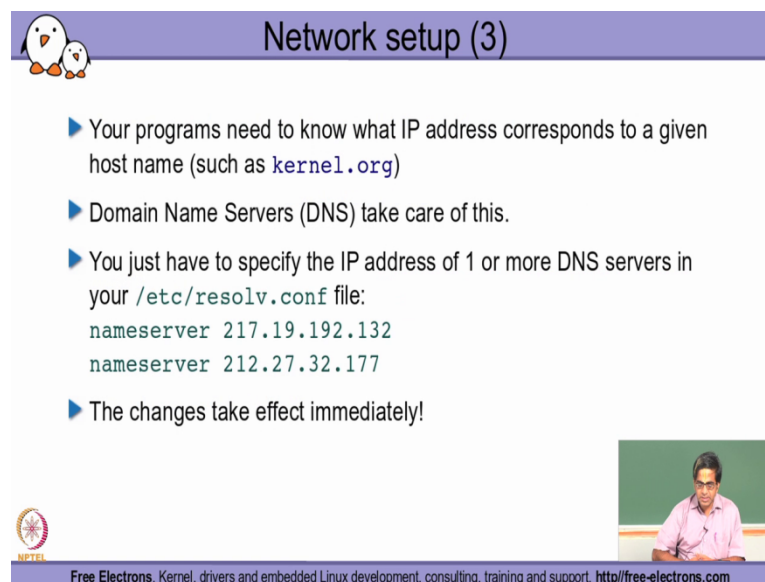
So this basically gives me the mechanism by which I will be able to find out what are all the different routes that are configured on my system among these configured routes I will also be able to find out what is the default gateway, because one of the routes will be explicitly marked as the default in my table of routes. So that entry will be taken as the Default gateway for all the packets that is actually coming out of this system into the network.

Suppose if I want to delete the route so I have a option by which I could specify del is the operation to the route command so here we said that we want to add we want to give an operation of an add to the route command here if you want del instead of add we say del of

the route and what do we want to route? What do we want to delete here which route we want to delete so it could either be the default route the default gateway that was previously configured with this command or it could be any other route and we could specify the corresponding IP here.

So route del of this particular network will delete that particular route in my list of routes that is available on the system. So the set of routes is basically what determines how my packet is actually going to go on into the system. So we will actually be talking about the routing part of it as a subsequently in the course when we give you a very brief overview about the network layer in our stats.



(Refer Slide Time: 09:44)



**Network setup (3)**

- ▶ Your programs need to know what IP address corresponds to a given host name (such as `kernel.org`)
- ▶ Domain Name Servers (DNS) take care of this.
- ▶ You just have to specify the IP address of 1 or more DNS servers in your `/etc/resolv.conf` file:

```
nameserver 217.19.192.132
nameserver 212.27.32.177
```
- ▶ The changes take effect immediately!

Free Electrons. Kernel, drivers and embedded Linux development, consulting, training and support. <http://free-electrons.com>

So the next configuration that we need to typically understand is how can we actually set up the remaining part of the network, so once we actually set up the IP address that particular port is said to become alive. So till its IP address is saved and explicit bring up to that particular interface to the `ifconfig up` command is done that particular interface is not at currently up and running. Once that is done like interface is all ready but it has to be now exclusively told what is the next interface to which the packets have to be sent by this guy and that is basically what we did with the route command.

Now once the route command is also established successfully the physical connectivity is there, the next thing we need to know is what is called as the name server configuration? So the Domain name server DNS is a protocol that actually takes care of it where there has to be

some person some protocol that is running to translate a machine name into corresponding IP address and which is that is basically the DNS server. So on my local system I typically configure the DNS server IP addresses in a particular file so that whenever any networking application is run on my system they basically go and look at this particular file and the DNS client which will start transparently running on my system will know what are the DNS server IP addresses in which this particular name the domain name or the machine name that is given by this application can be used for resolving the name to the IP address.

So we just talked about the example of giving a URL in a browser p let us say [www.yahoo.com](http://www.yahoo.com). My network layer in my stack is not going to understand the English machine name or Domain name or yahoo.com. It needs to understand it basically understands only the IP addresses. So somebody has to translate from the domain name of yahoo.com to the corresponding IP addresses and that person who is doing this translation is what is called as a DNS server DNS servers available and that's basically what we called resolved available in the etc directory in all the configuration file system to function normally is available right ?

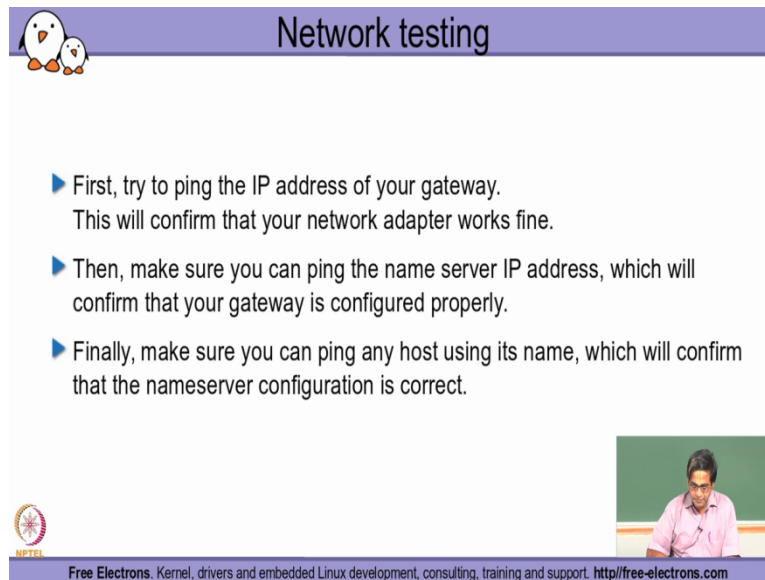
So in the etc directory there is a file called result.com in which we could actually have a list of name servers listed one name server per line unspecified what are those corresponding name server IP addresses so anytime whenever there has to be a domain name of a hostname that has to be converted that has to be resolved to a corresponding IP address of that particular name first line in which I specified the name server and followed with IP address.

That particular server IP will be contacted and given a request for doing this resolution if that is failing for some reason so that that particular Server is not contactable not reachable for whatever reason I could also have any number of fallback options of name server configuration done the same file so if for example the first name server 2.2 17 dot 19.1 92.1 32 is not reachable at any instant of time automatically and transparently the 13:28 destroyer that will be run on my system currently will go and try to resolve the name to the IP address by contacting the second server that has been listed here.

So the name servers a keyboard so following the name server keyword I specify what is a DNS server IP and likewise I could have multiple name server is configured in my rusalt.com 5 for fault order and purposes so just in case my first DNS Server is not contactable or not reachable or is not giving me the response back, automatically I will have my DNS client

contact the next name server that has been configured in this file and so on till it finally successfully gets the resort IP address for that particular name, right?

(Refer Slide Time: 14:16)



The slide is titled "Network testing" and features a header with a penguin icon. It contains a list of three steps for network testing, each preceded by a blue arrow icon. At the bottom right, there is a small video inset showing a man in a pink shirt speaking. The footer includes the NETEL logo and the text "Free Electrons. Kernel, drivers and embedded Linux development, consulting, training and support. <http://free-electrons.com>".

- ▶ First, try to ping the IP address of your gateway.  
This will confirm that your network adapter works fine.
- ▶ Then, make sure you can ping the name server IP address, which will confirm that your gateway is configured properly.
- ▶ Finally, make sure you can ping any host using its name, which will confirm that the nameserver configuration is correct.

So in terms of troubleshooting what should be actually first try to do we need to run a command called ping, so we tried to basically whenever we find that we are not able to access a particular server on the network, we first try to trouble shoot it in the local network by trying to do something called as a ping, right?

So ping essential is a command is used to find out if a particular mission is reachable or not on the network. So when in a particular remote pressure is not reachable it is not necessary always that the remote machine alone is down or inaccessible right now. So I could actually have the problem anyway in my network path so typically what we do is, we first try to ping the IP address of the Gate way that has been configured for that particular interface, right?

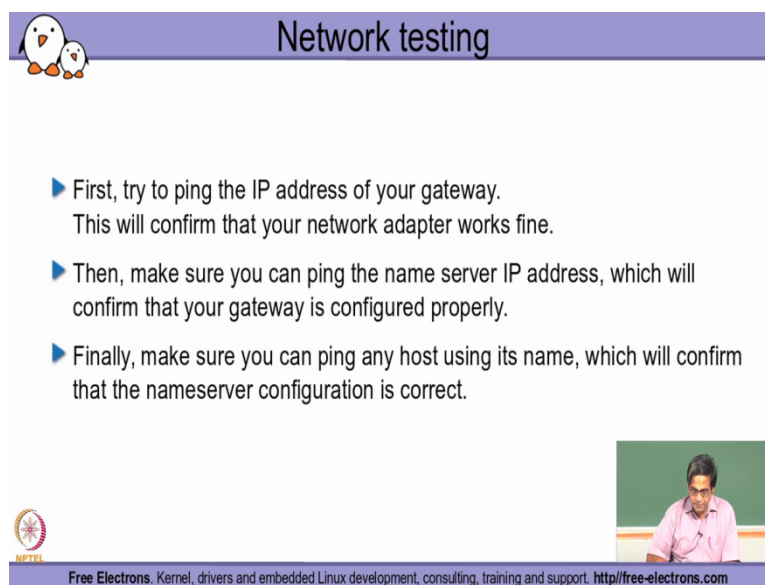
So just a few slides back we configure the gateway IP address, so we tried to ping that particular Gateway IP address to see if our local Gateway is reachable or not right? So assuming that is reachable then we basically try to find out if our name server IP address is reachable or not. So if the gates for example not reachable then we know definitely the problem is somewhere isolated in our Local Network alone because of which package is not even able to go to the next hop, right?

Now if that is reachable then we try to find out if my DNS server is reachable by trying to ping the name server IP address that was configured inresult.con file right? Now if that is





reaching successfully. What this basically proves is that even my Gateway is configured correctly, because of which packets are able to get out of my Gateway that is typically my local network most of the time and then reachable the Internet successfully because most of the times again my name server resolution IP address will be an IP address which is available only in the public Internet right? or at least it will be the IP address which is actually placed in my ISP site right?

(Refer Slide Time: 16:30)



**Network testing**

- ▶ First, try to ping the IP address of your gateway.  
This will confirm that your network adapter works fine.
- ▶ Then, make sure you can ping the name server IP address, which will confirm that your gateway is configured properly.
- ▶ Finally, make sure you can ping any host using its name, which will confirm that the nameserver configuration is correct.

Free Electrons. Kernel, drivers and embedded Linux development, consulting, training and support. <http://free-electrons.com>

Now if this is also reachable then we know accessing the Internet is seem to be fine then we can possibly say that there is a problem somewhere in the path from our ISP entry point to any of the hopes it takes to reach the final Destination right? So in this way we will be able to sort of troubleshoot to a minimal extent of where the problem could be really present whenever we are not able to successfully reach the Final Destination machine.

So the problem could be either in our own local system the problem could be alternatively in our Gateway, the problem could be in my name server IP address that I have configured in my rusal.com file locally and if there is no problem in any of this and most possibly the problem could be in any of the network hope paths that my path that my package is actually taking after the ISP is entry point to the Final Destination right?

So there by we basically try to get an idea of where the problem could typically happen by doing sort of an elimination of trying to test our reach ability right from our Local Network to

the remote right up to the remote system and sort of isolate where exactly a problem could be lying whenever we find that a remote system is not reachable from our local system.

Thank you!