

**Lab Assessment-1**

**Subject-Network and Communication**

**Name-Avnish Tiwari**

**Reg.No-19BCE0634**

**Slot-L25+L26**

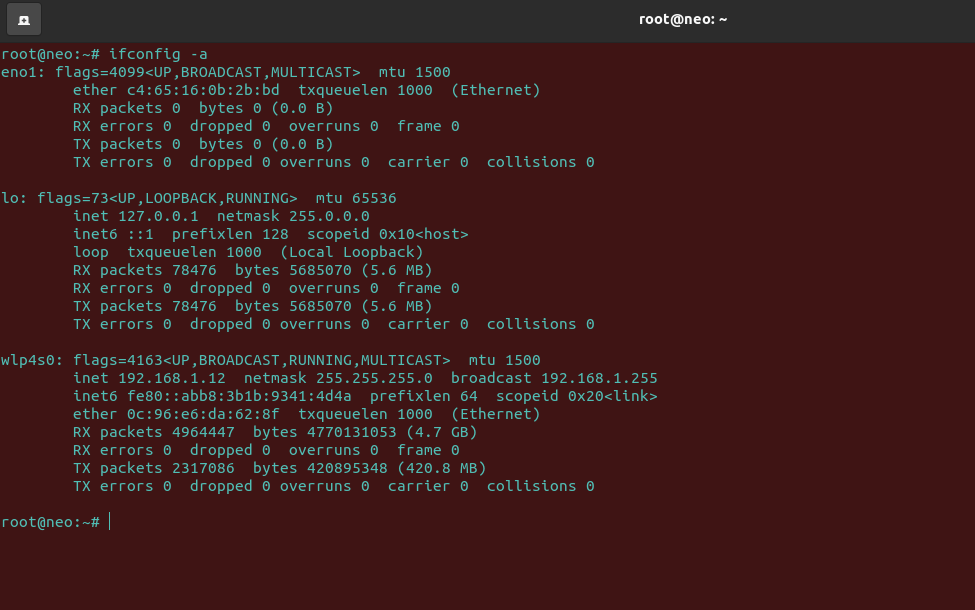
**Activity 1**

**1.Ifconfig**

1. **Option Used: -a**

* **Option Description:**

**This option tells ifconfig to show information about all interfaces, both active and inactive.**

* **Screenshot of output:**
* **Your own interpretations of the obtained results for each option:**

**When we use this option we find that it returns all the detailed information of interfaces whether they are active or inactive.**

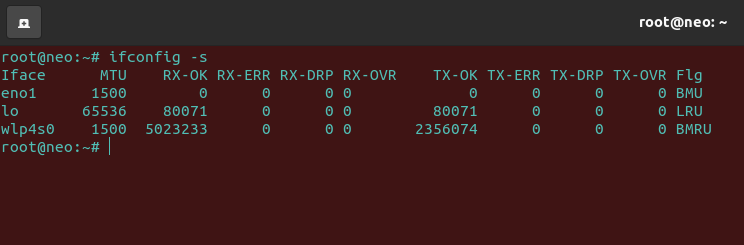
**This can be primarily used when we want to see the detailed information and not just summary.**

1. **Option Used: -s**

* **Option Description:**

**This is the "short listing" option, which shows a one-line summarized listing of data about each interface.**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

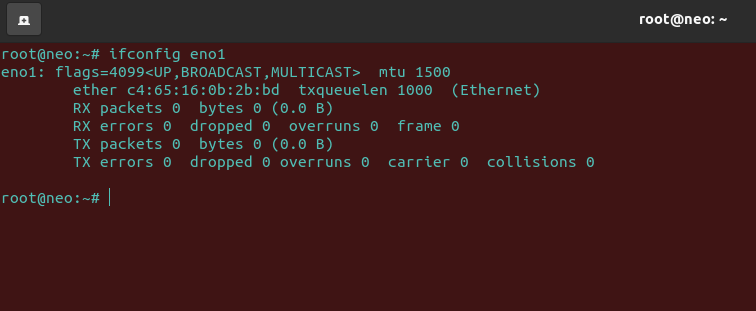
**This is a very interesting option as the information returned is about interface activity, and not configuration,so it gives the user a basic summary and that is very useful.**

1. **Option Used: [int]**

* **Option Description:**

**Using interface names (like eno1) as an argument with the “ifconfig” command will display details of specific network interfaces.**

* **Screenshot of output:**

****

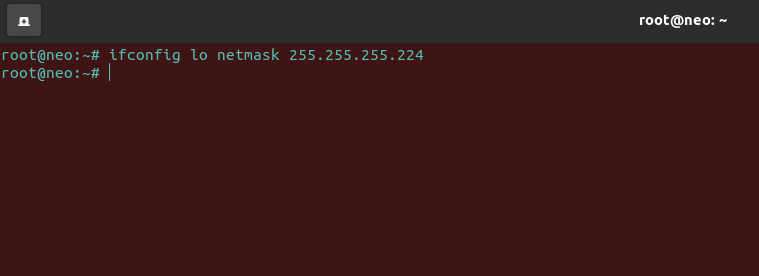
* **Your own interpretations of the obtained results for each option:**

**It is a very helpful option as just simply follow up your ifconfig command with the name of an interface to get only information about that interface. For instance, you could issue the command ifconfig eno1 if you only wanted information about the eno1 interface, and not the other interfaces.It saves a lot of time as we just get information of what we want.**

1. **Option Used: netmask [addr]**

* **Option Description:**

**Using the “ifconfig” command with “netmask” argument and interface name as (lo) allows you to define an netmask to an given interface.**

* **Screenshot of output:**
* **Your own interpretations of the obtained results for each option:**

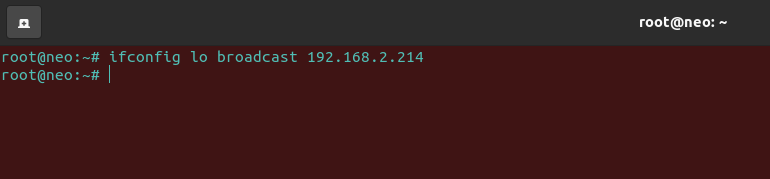
**Using the "netmask" option allows you to set the network mask for a given interface. For instance, setting the network mask for lo could be done by entering ifconfig lo netmask 255.255.255.224**

1. **Option Used: broadcast [addr]**

* **Option Description:**

**Using the “broadcast” argument with an interface name will set the broadcast address for the given interface.**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**When the "broadcast" option is accompanied by an address argument, as in ifconfig lo broadcast 192.168.2.214, then the broadcast address for the specified interface will be set.**

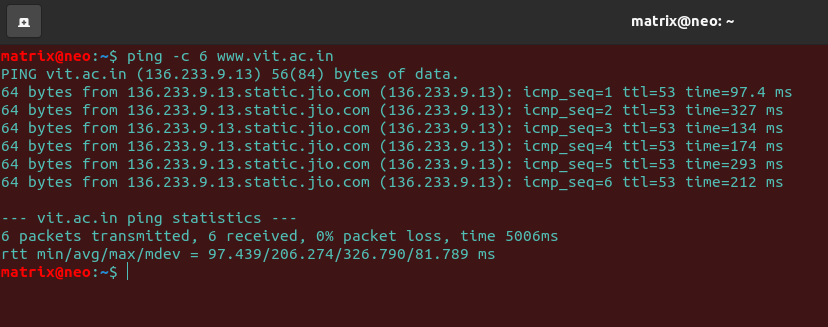
**2.Ping**

1. **Option Used: -c [number of requests]**

* **Option Description:**

**You can specify the number of requests to be sent after which ping exits, using the -c flag as shown**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

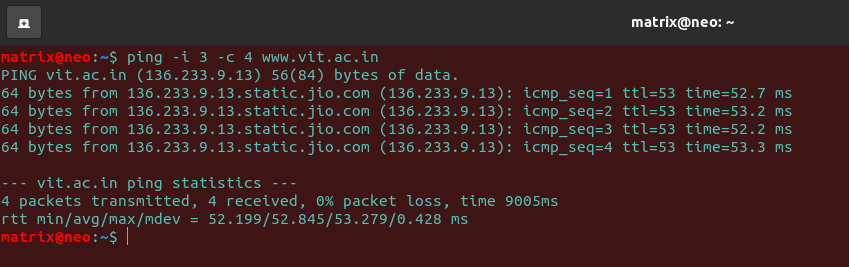
**This is a nice feature to use as you can preset the number of cycles which is very convenient rather than forcing the process to stop abruptly.**

1. **Option Used: -i**

* **Option Description:**

**It sets the Time when To Live**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**The -i flag allows you to set an interval in seconds between sending each packet, the default value is one second.**

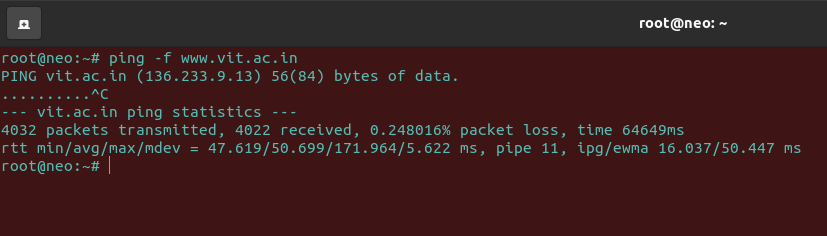
**Like in the above example we set the number of packets to 4, and the time interval being 3 seconds,so the 1st packet is transmitted and received and then we wait for 3 seconds for the next packet to be transmitted.**

1. **Option used: -f**

* **Option Description:**

**It is used as a flood ping which sends requests as fast as possible to determine the response of our network under high-load conditions.**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**We see that this command tells us the statistics of the website we have used.**

**This command is helpful in determining our network response when the load on the website is very much.**

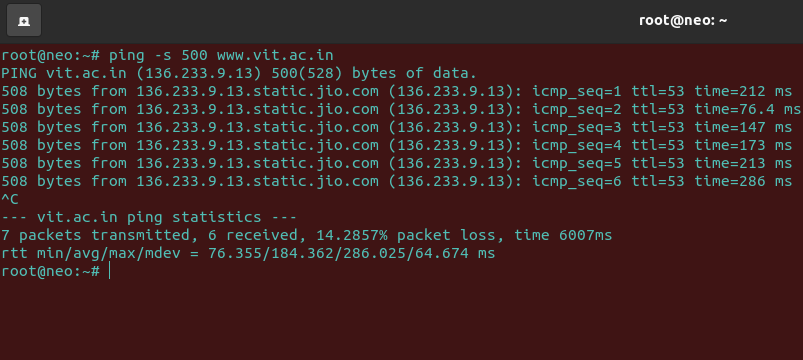
**It gives us information about the number of packets transmitted,number of packets received,the packet loss,time in ms,pipe value and the min,avg,max and standard deviation of the round trip time(rtt).**

1. **Option Used: -s**

* **Option Description:**

**It increases the size of the payload to your wish.**

* **Screenshot of output:**

****

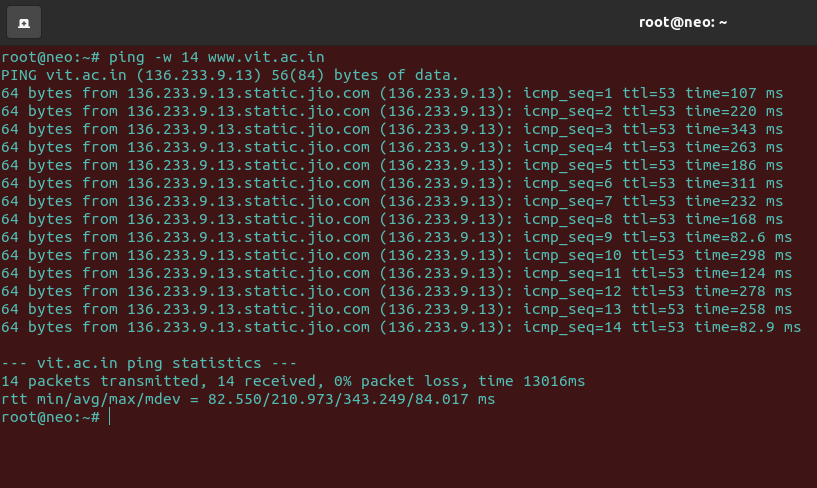
* **Your own interpretations of the obtained results for each option:**

**The default packet size should be sufficient for a ping test, however, you can change it to meet your specific testing needs.So we change it and can see 508 bytes are transferred.The extra 8 bytes are because of the ICMP header.**

1. **Option used: -w**

* **Option Description:**

**It sets a timeout in seconds before ping exits.**

* **Screenshot of output:**

* **Your own interpretations of the obtained results for each option:**

**As we can see in this screenshot,regardless of how many packets have been sent or received,the ping exits.**

**It is helpful like we can set the time and then we don’t have to end the command forcefully.**

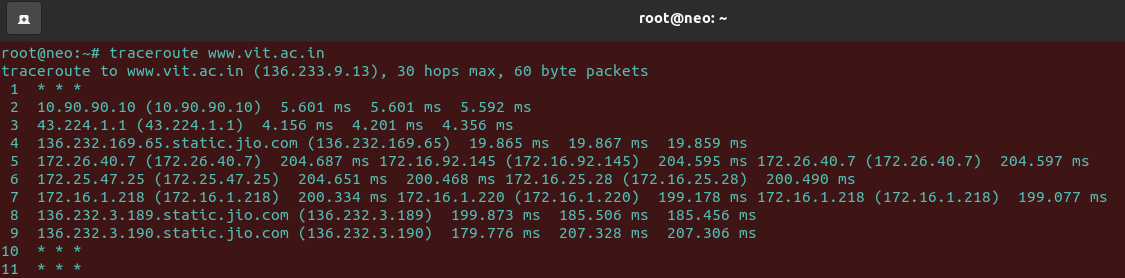
**3.Traceroute**

1. **Option Used:- traceroute <server-name>**

* **Option Description:**

**The server-name above is the destination name or IP address. For example, traceroute is used to find the network path from our machine to** [**www.vit.ac.in**](http://www.vit.ac.in)

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**Each line gives the details of interaction with each router encountered. So we see that traceroute not only gives the IP addresses of the intermediate routers but also three round trip times for that particular router as for each router the traceroute commands fires three packets.**

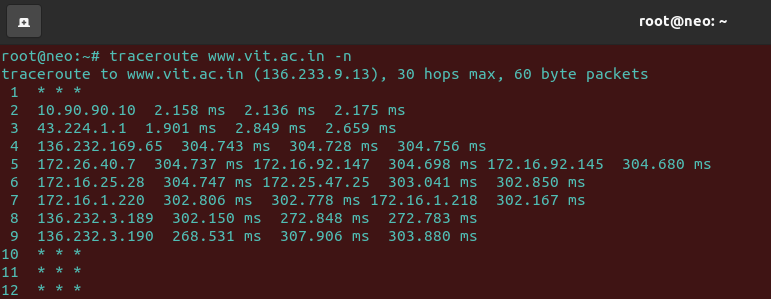
**Also you see some ‘\*’ on some lines.Basically This depicts that the required field could not be fetched. The reason can be anything from reverse DNS lookup failure to packets not hitting the target router to packets getting lost on their way back.**

1. **Option Used: -n**

* **Option Description:**

**Traceroute provides an option through which the mapping of IP addresses with host name (that traceroute tries) is disabled. The option for doing this is ‘-n’ .**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

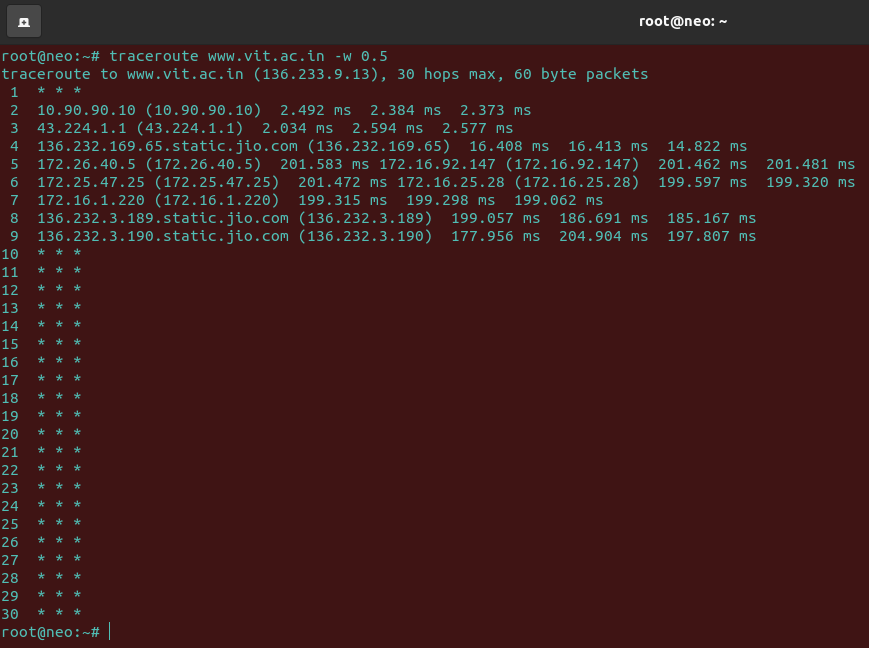
**As we can see in the above screenshot,there is no host name displayed in the output.**

1. **Option Used: -w**

* **Option Description:**

**Configure Response Wait Time-This traceroute utility waits after issuing a probe can also be configured.**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**As we see in the above Screenshot,the -w option expects a value which the utility will take as the response time to wait for. In this example, the wait time is 0.5 seconds and the traceroute utility was unable to wait for any response and it printed all the \*’s.**

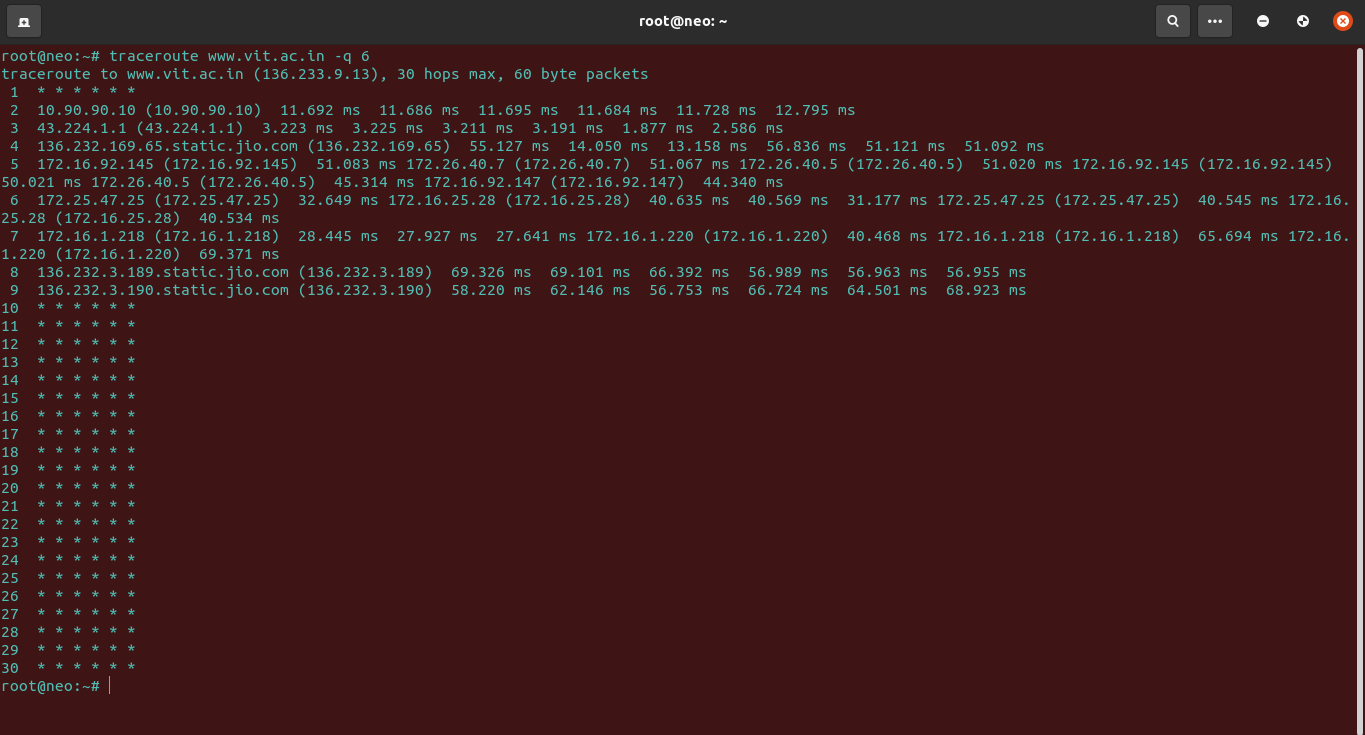
**So we see that traceroute tried 30 attempts (the max hop attempts) and then gave up as no ICMP packet was received in 0.5 seconds.**

1. **Option Used: -q**

* **Option Description:**

**Configure Number of Queries per Hop**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**As we know beforehand, the traceroute utility sends 3 packets per hop to provide 3 round trip times. This default value of 3 is configurable using the option ‘-q’.**

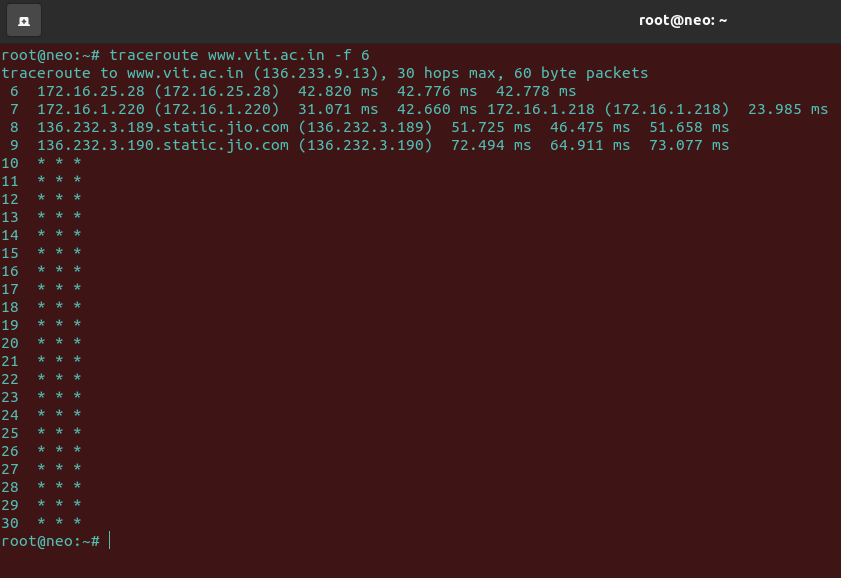
**So we see that in the above example after configuring the number of probes to 6, the output started showing six round trip times per hop.**

1. **Option Used: -f**

* **Option Description:**

**Configure the TTL value to start with**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**We know that the default value of TTl is 1 which means it starts off with the first router in the path but using the ‘-f’ option a new value of the TTL field can be set.**

**So we see in the screenshot that after using the -f option with value 6, only the last (6th) line from the previous output was shown.**

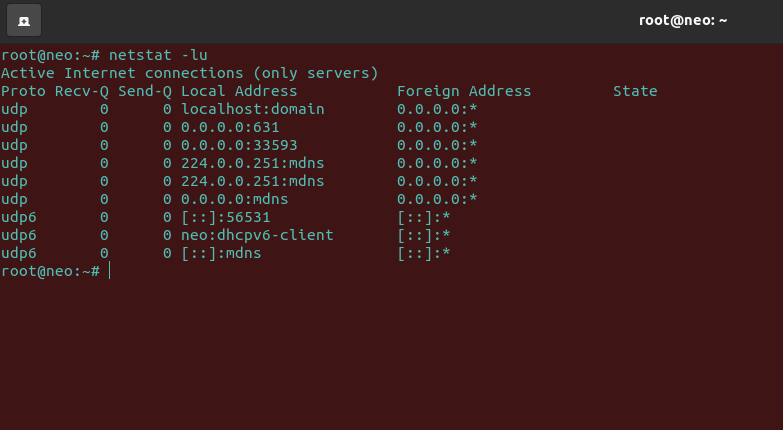
**4. Netstat**

1. **Option Used: -lu**

* **Option Description:**

**Listing all active listening UDP ports by using option netstat -lu.**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

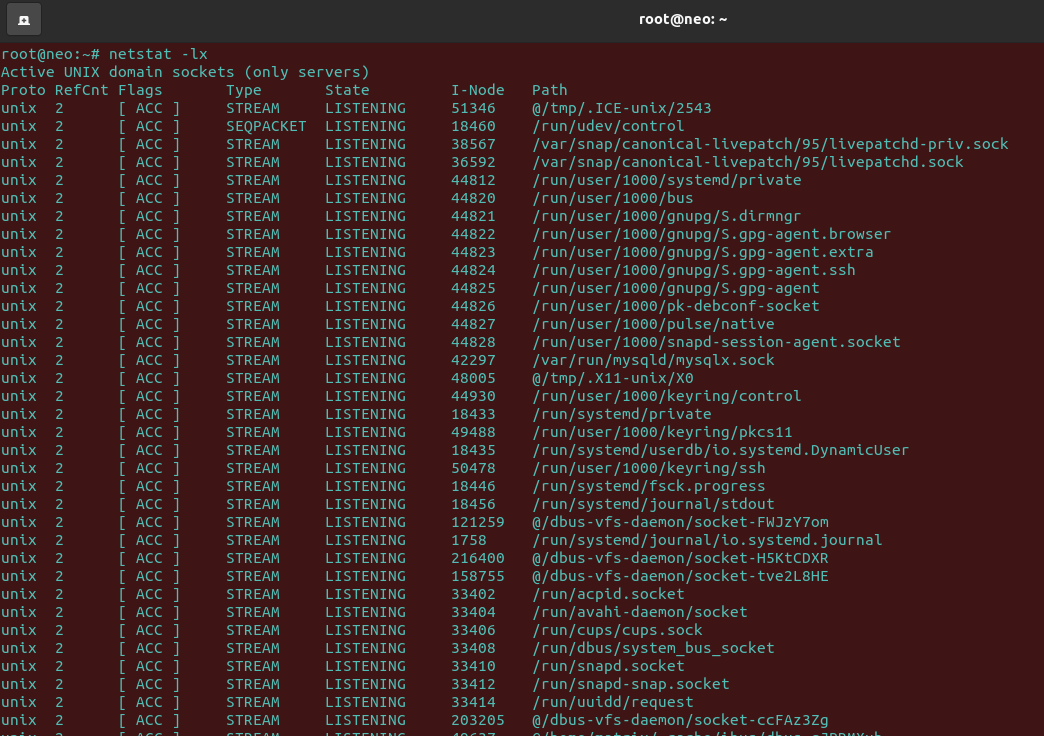
**As we see in the above screenshot,only the active listening UDP ports are shown with its local and foreign address.**

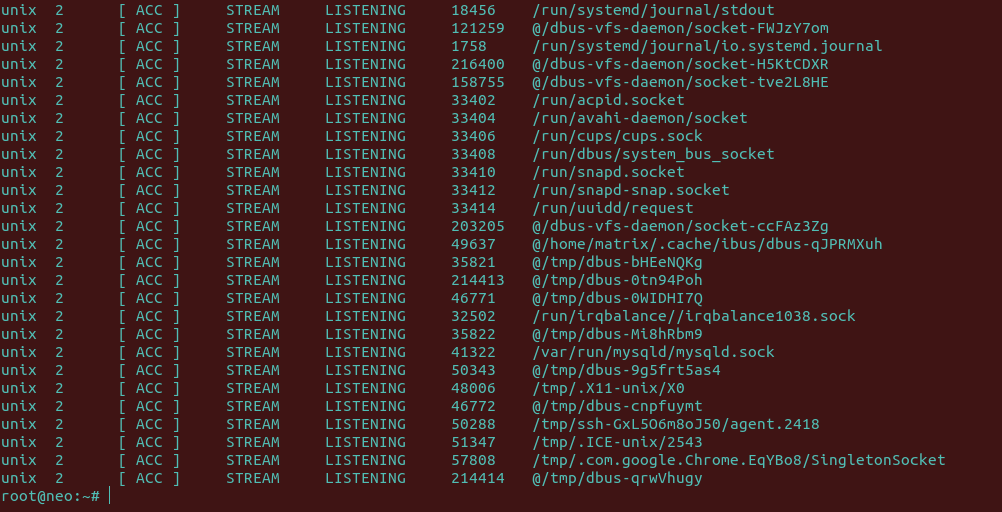
1. **Option Used: -lx**

* **Option Description:**

**Listing all active UNIX listening ports using netstat -lx.**

* **Screenshot of output:**

****

****

* **Your own interpretations of the obtained results for each option:**

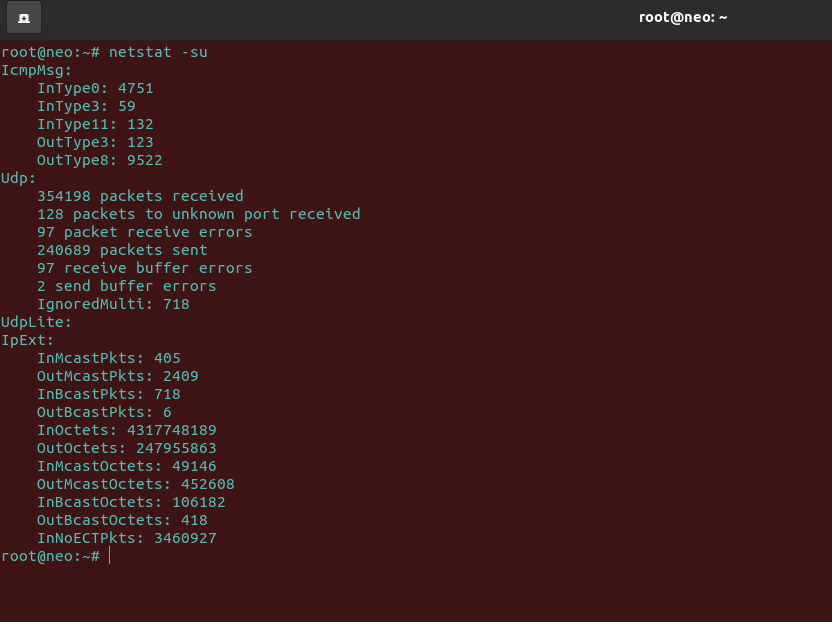
**As we can see from the above screenshot,this option separates the active UNIX ports from others and give information about reference count,flags,type,state, I-node and path.**

1. **Option Used: -su**

* **Option Description:**

**Showing the Statistics by UDP Protocol**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

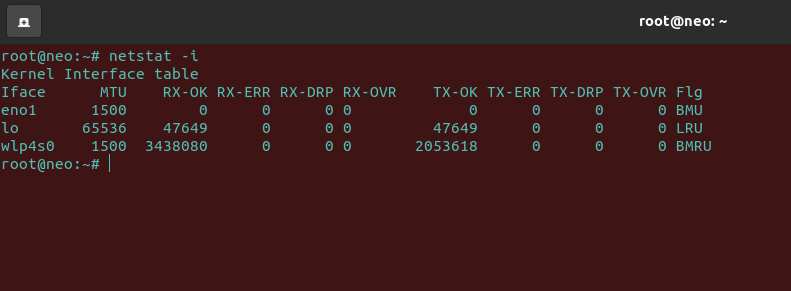
**As we can see in the above screenshot,this function separates the UDP protocol from other protocols that include TCP,ICMP and IP protocols and then shows the statistics of the UDP protocols.**

1. **Option Used: -i**

* **Option Description:**

**Show the list of network interfaces**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**As we can see in the above screenshot,It Shows network interface packet transactions including both transferring and receiving packets with MTU size.**

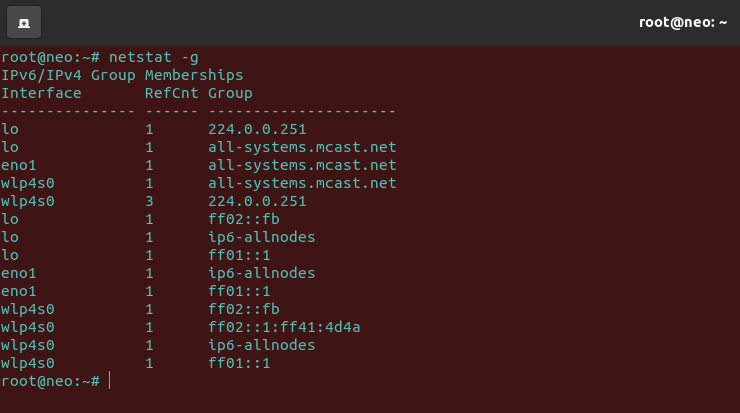
**It is a bit similar to ifconfig.**

1. **Option Used: -g**

* **Option Description:**

**It Displays IPv4 and IPv6 Information**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**As we can see from the above screenshot,it displays multicast group membership information for both IPv4 and IPv6.**

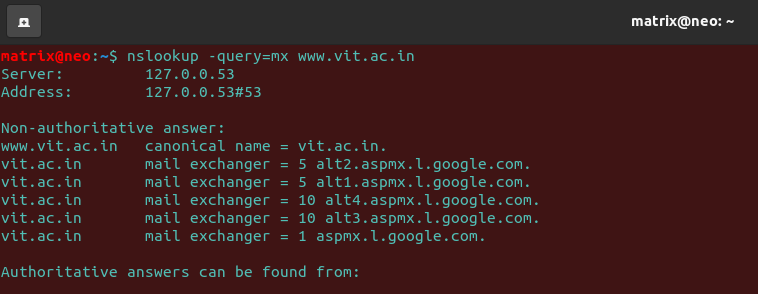
**5.Nslookup**

1. **Option Used: -mx**

* **Option Description:**

**MX ( Mail Exchange ) record maps a domain name to a list of mail exchange servers for that domain. The MX record tells that all the mails sent to “@vit.ac.in” should be routed to the Mail server in that domain.**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

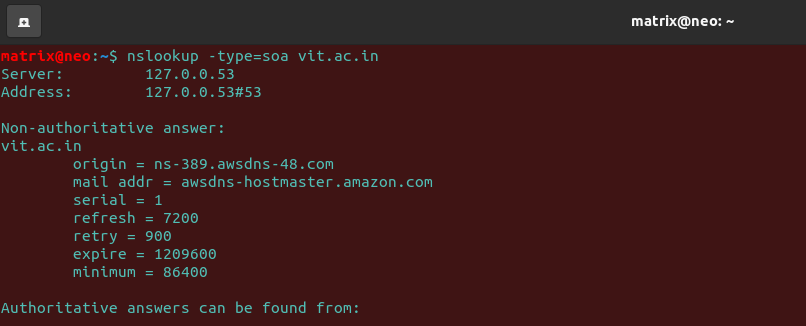
**In the above example, we have 5 MX records for the domain “vit.ac.in”. The numbers ( 1,5, 10 ), associated with the MX records, tell the preference of the mail server. Lower the number, higher the preference.**

1. **Option Used: soa**

* **Option Description:**

**You can query and display the SOA (Start of Authority) record with nslookup by specifying the type of query.**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

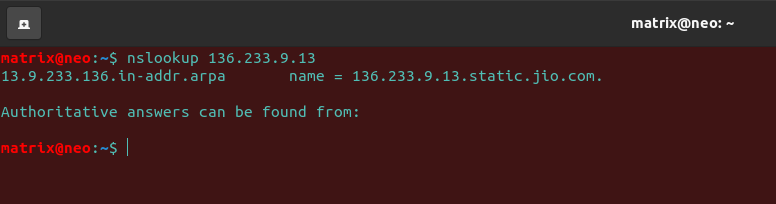
**From the above screenshot we can see that SOA record ( start of authority ), provides the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number,mail address,serial,refresh,retry,expire and minimum.**

1. **Option Used: nslookup [ipaddress]**

* **Option Description:**

**Reverse DNS lookup**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**We can see from the above screenshot that we can do the reverse DNS lookup and search for the domain name associated with an IP address.The IP address can be founded by simply typing- “nslookup vit.ac.in”**

1. **Option Used: any**

* **Option Description:**

**View available DNS records using -query=any**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

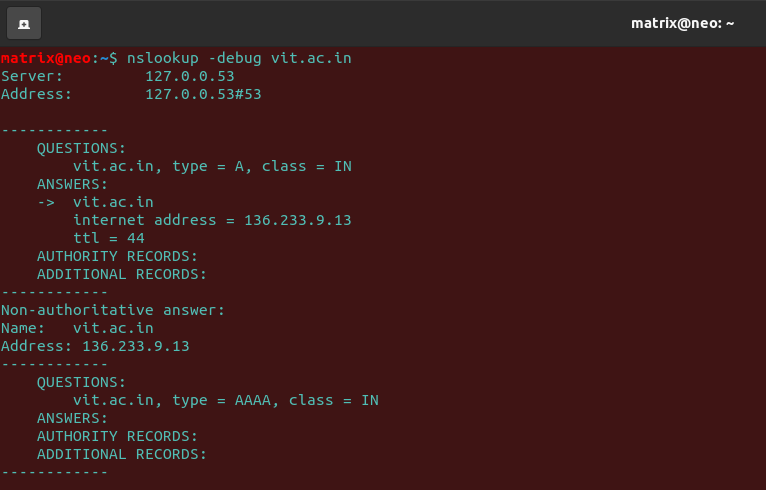
**You can display all the above records (that are set) in one single command using the any option and as we can see from the above screenshot, you’ll see a consolidated output of all above commands.**

1. **Option Used: debug**

* **Option Description:**

**Enabling debug mode using -debug**

* **Screenshot of output:**

****

* **Your own interpretations of the obtained results for each option:**

**As we can see in the above screenshot,this command will display the packets information during searching.**

**Activity-2**