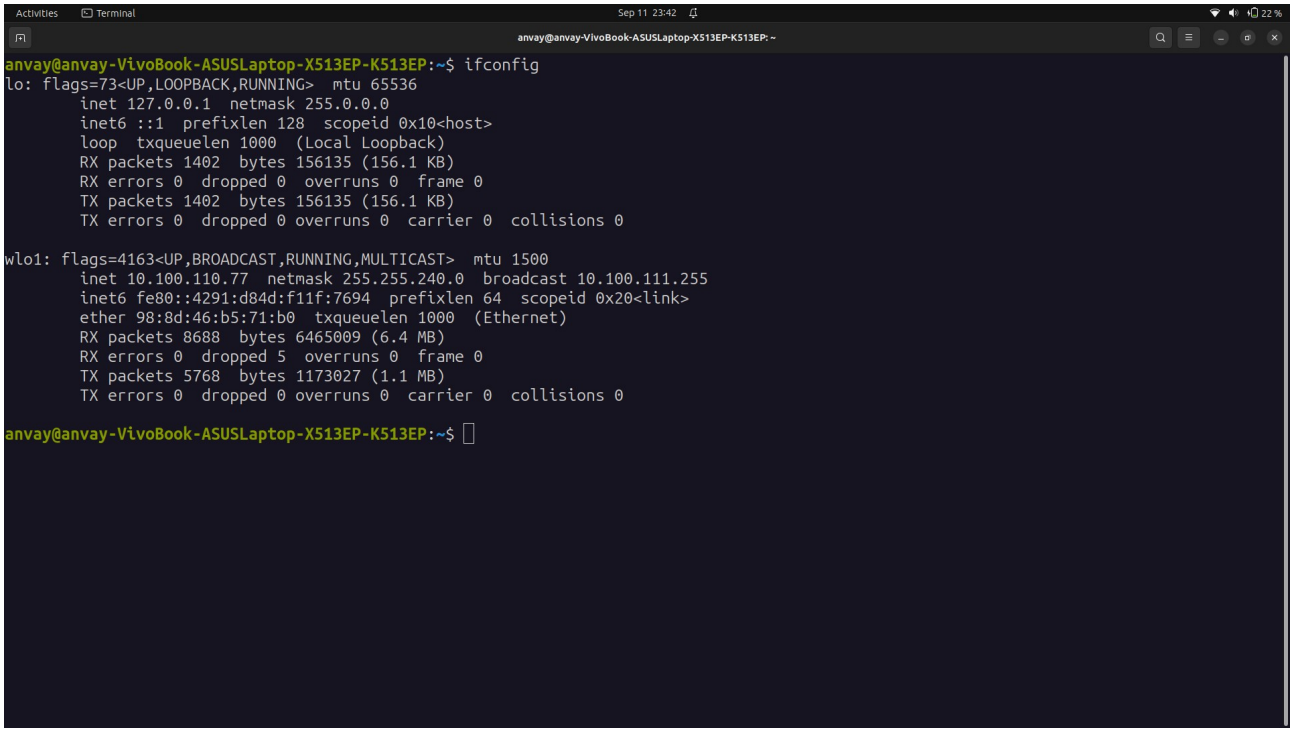
CN Assignment-2

MIS: 112103059
TY Comp div-1
Batch: T3

1. ifconfig



DESCRIPTION

Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.

If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

2. ip

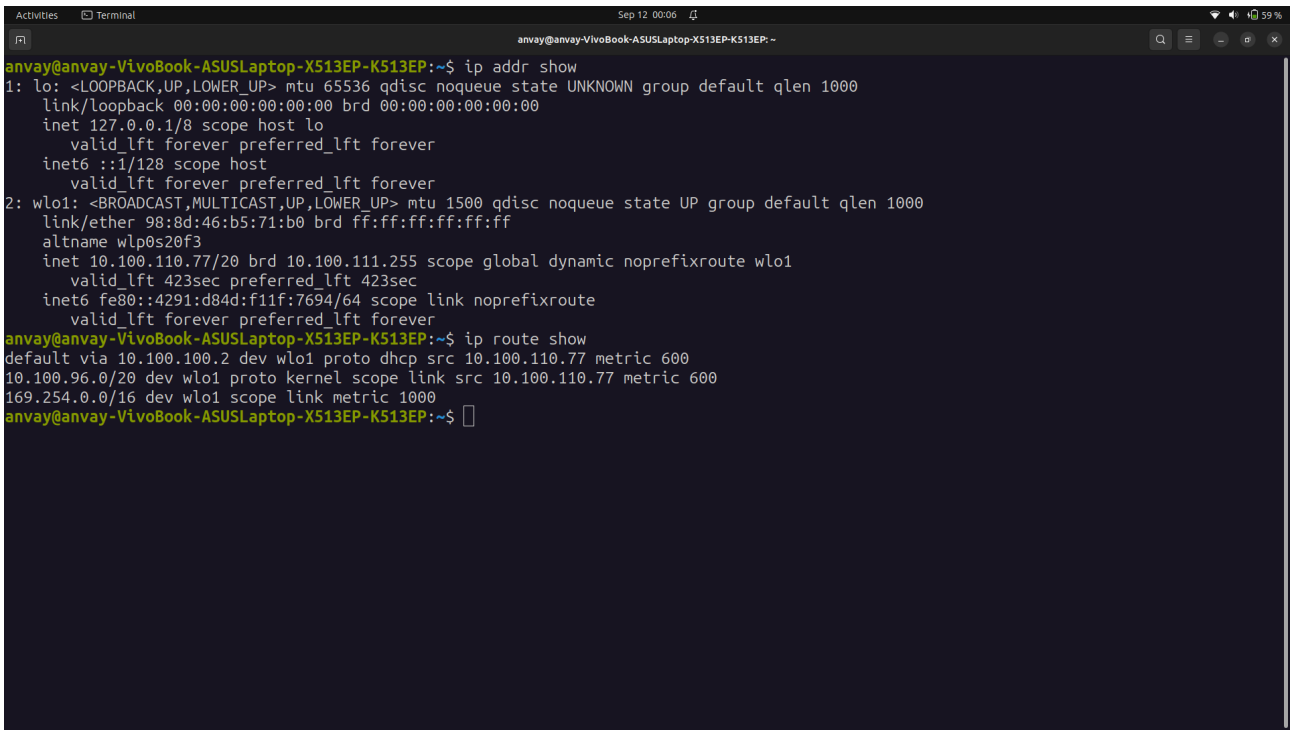
DESCRIPTION

The `ip` command in Linux is a powerful and versatile utility for configuring and managing network interfaces, routes, and related networking information.

Options:

addr show: To display information about all network interfaces, their IP addresses, and other details:

route show: To view the routing table:



3. traceroute

The traceroute command in Linux is used to trace the route that packets take from your computer to a destination host or IP address on a network. It helps you visualize the path that network packets follow through routers and network devices, showing the IP addresses of each intermediate hop and the time it takes for a packet to travel from your computer to that hop.

Options:

`-n`: Display numeric IP addresses instead of resolving hostnames (useful for faster execution).

`-q <number>`: Set the number of probe packets per hop (default is 3).

`1`: This indicates that this is the first hop in the traceroute.

`_gateway`: This is the hostname or identifier for the first hop, which is often the default gateway or router in your local network.

`(192.168.180.64)`: This is the IP address of the first hop, which is typically a router in your local network.

`1.863 ms`: This is the round-trip time (latency) for the first hop, measured in milliseconds. In this case, it took approximately 1.863 milliseconds to reach the first hop.

`!N`: This `!N` represents a "network unreachable" message. It indicates that the network path to the destination is not reachable at this hop. It might be due to network configuration, routing issues, or firewall rules preventing the traceroute packets from reaching the destination.

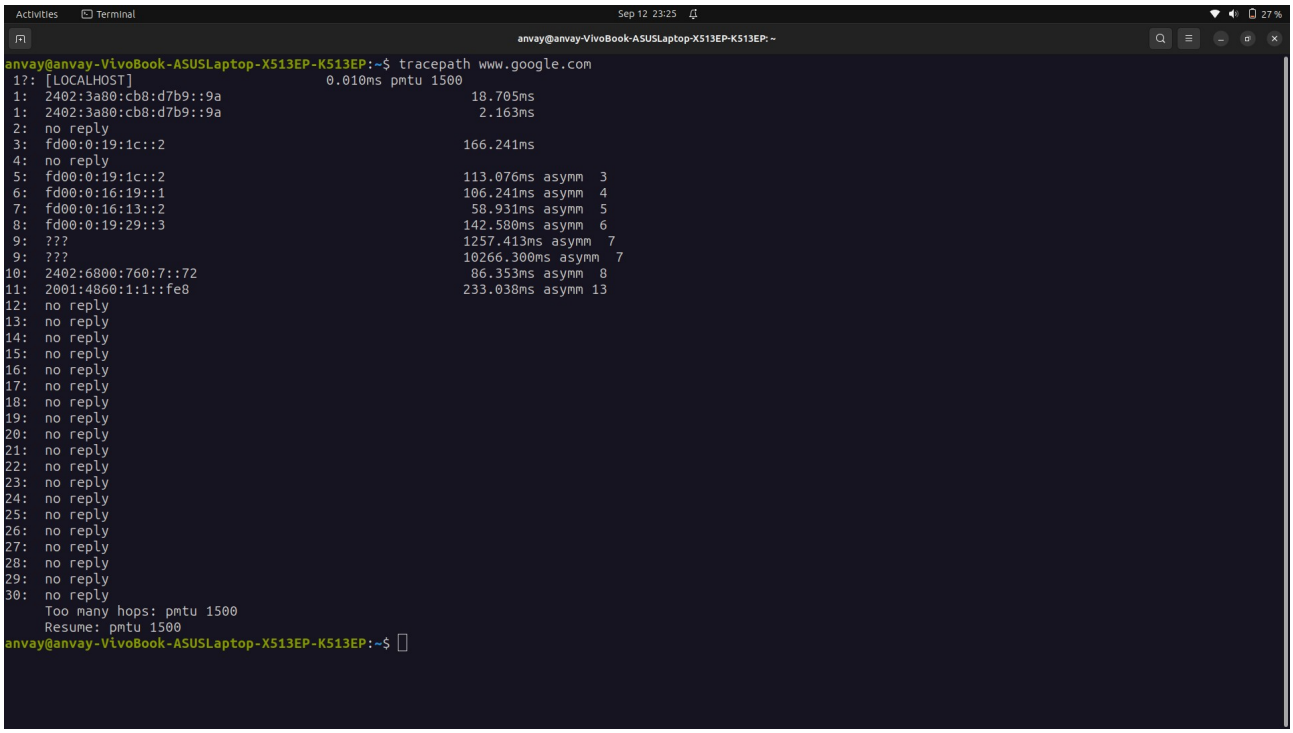
`1.869 ms`: This is the round-trip time for the second probe to the same hop, which is similar to the first probe.

`!N`: Again, this indicates a "network unreachable" message for the second probe.
`*`: An asterisk (*) represents that the third probe to the same hop did not receive a response.

4. tracepath

DESCRIPTION

The `tracepath` command is a Linux utility that is used to trace the path that network packets take from your computer to a destination host or IP address on a network, similar to the `traceroute` command. It helps you visualize the route that packets follow through routers and network devices. The primary difference between `tracepath` and `traceroute` is in the output format and some options.



The first column shows the TTL of the probe, followed by colon. Usually the value of TTL is obtained from the reply from the network, but sometimes it does not contain the necessary information and we have to guess it. In this case the number is followed by ?.

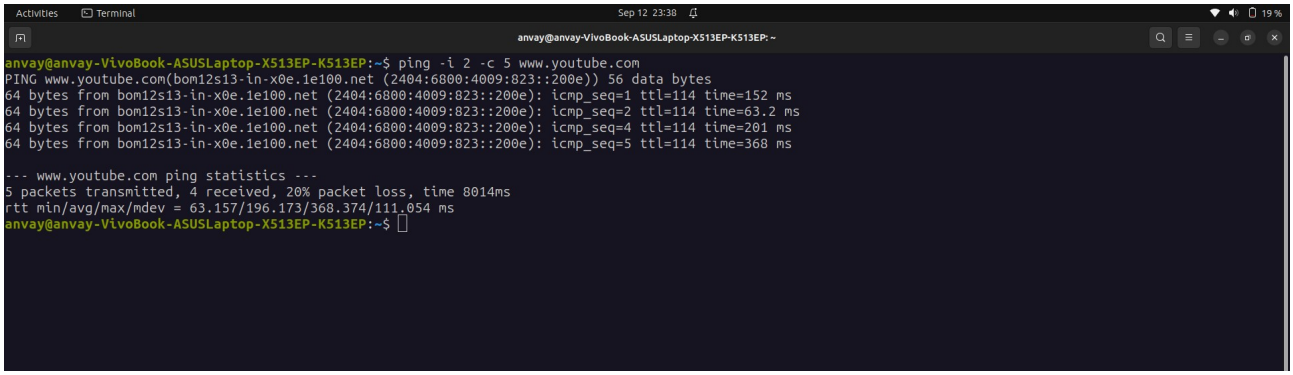
The second column shows the network hop which replied to the probe. It is either the address of the router or the word [LOCALHOST], if the probe was not sent to the network. The rest of the line shows miscellaneous information about the path to the corresponding network hop. It contains the value of RTT, and additionally it can show Path MTU when it changes. If the path is asymmetric or the probe finishes before it reaches the prescribed hop, the difference between number of hops in forward and return direction is shown next to the keyword "async". This information is not reliable, e.g. the

third line shows asymmetry of 1. This is because the first probe with TTL of 2 was rejected at the first hop due to Path MTU Discovery. The last line summarizes information about all the paths to the destination. It shows detected Path MTU, amount of hops to the destination and our guess about the number of hops from the destination to us, which can be different when the path is asymmetric.

5. ping

DESCRIPTION
The ping command in Ubuntu (and other Linux distributions) is used to test the reachability of a host (usually a computer or server) on an Internet Protocol (IP) network. It also measures the round-trip time for packets to travel from your computer to the target host and back. Here's how you can use the ping command in Ubuntu.

Options:
-i <interval>: Set the time interval (in seconds) between sending each ping packet (default is 1 second).
-c <count>: Specify the number of ping packets to send before stopping (default is unlimited).

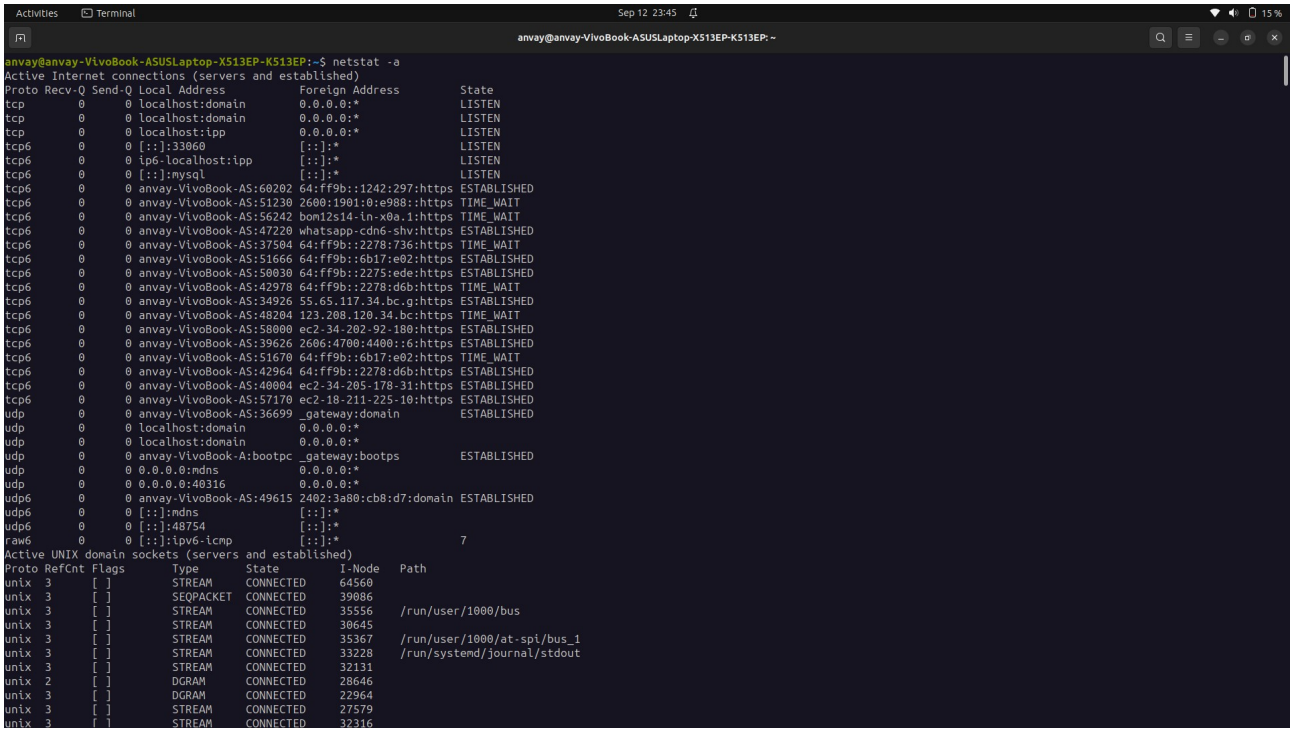


This command sent 5 ping packets to www.youtube.com with a 2-second interval between each packet and then stop. Out of 5 packets transmitted, only 4 were revieced.

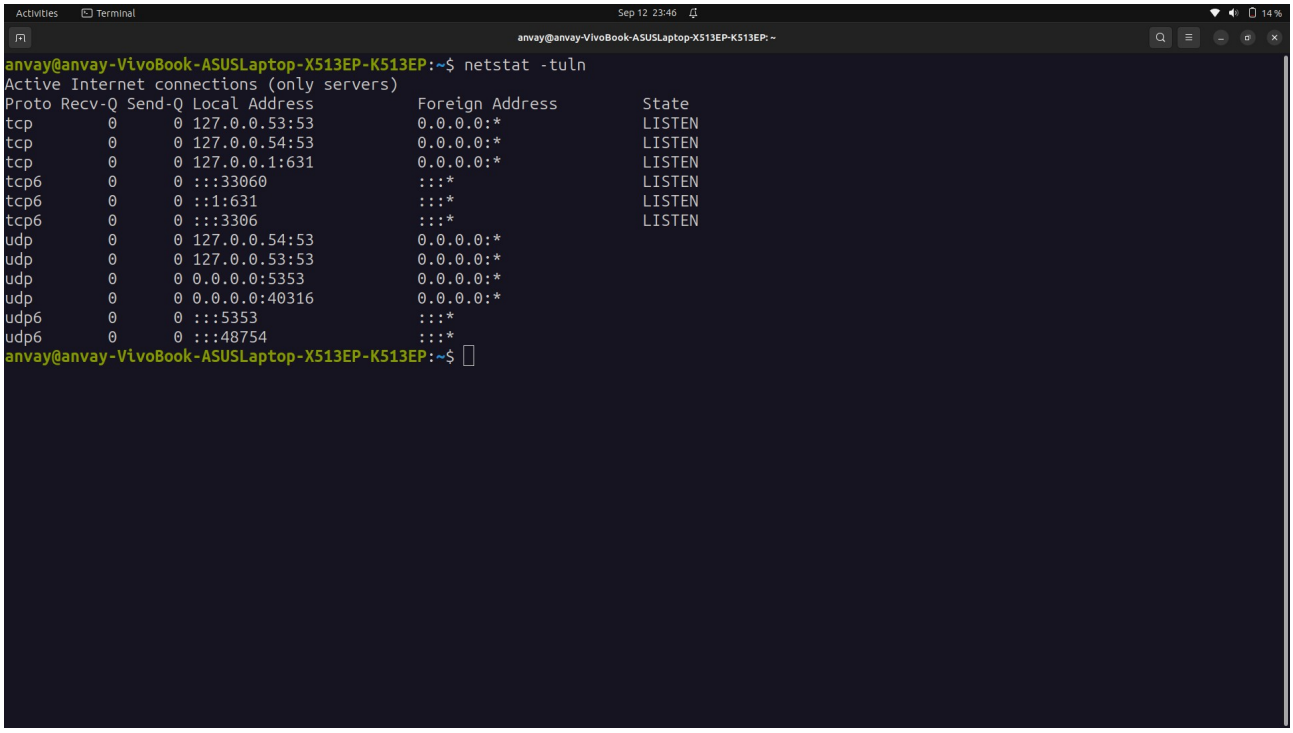
6. netstat
DESCRIPTION:
The `netstat` command is a network utility available on Linux and other Unix-like operating systems. It is used to display various network-related information, including network connections, routing tables, interface statistics, masquerade connections, and more. `netstat` can be a helpful tool for diagnosing network issues, monitoring network activity, and understanding network configurations.

OPTIONS:

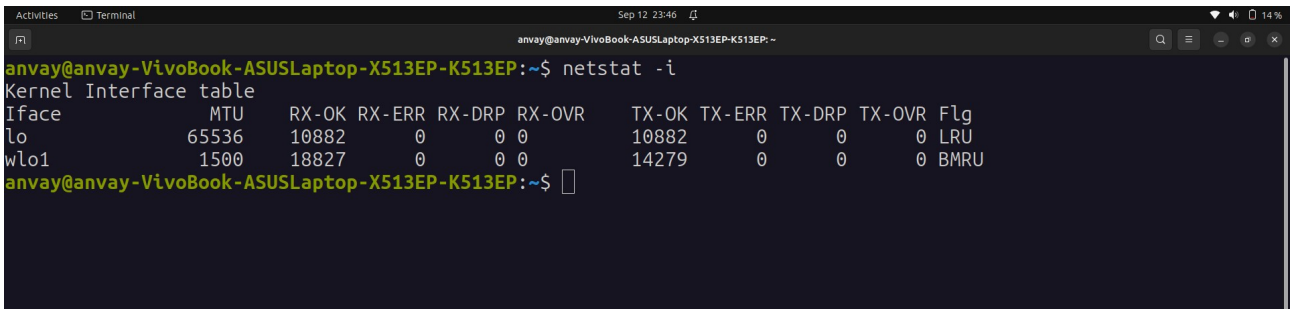
1. Display All Network Connections:



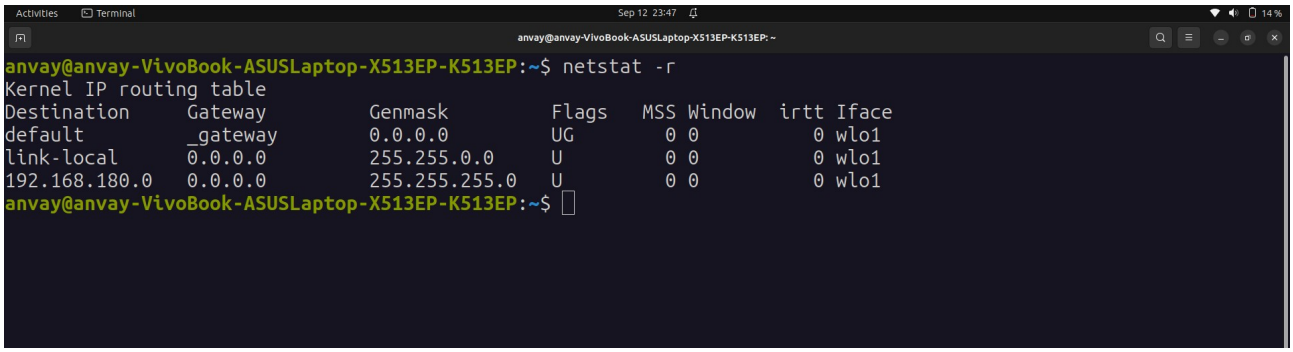
2. Display Listening Ports:



3. Display Network Statistics:



4. Display Routing Table:

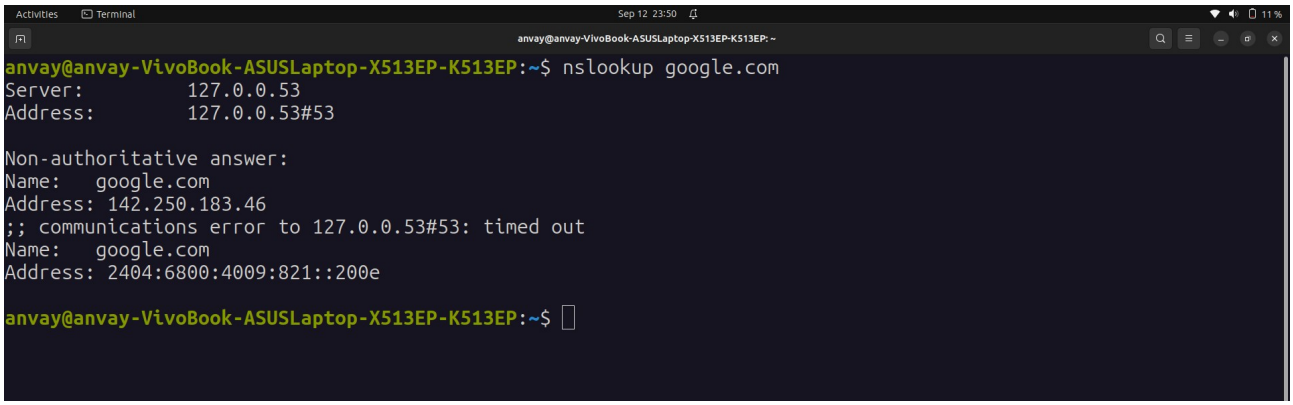


7. nslookup

DESCRIPTION:

The `nslookup` command is a network utility used for querying Domain Name System (DNS) servers to obtain information about domain names, IP addresses, and other DNS records. It is a valuable tool for troubleshooting DNS-related issues, checking DNS configurations, and resolving domain names to IP addresses.

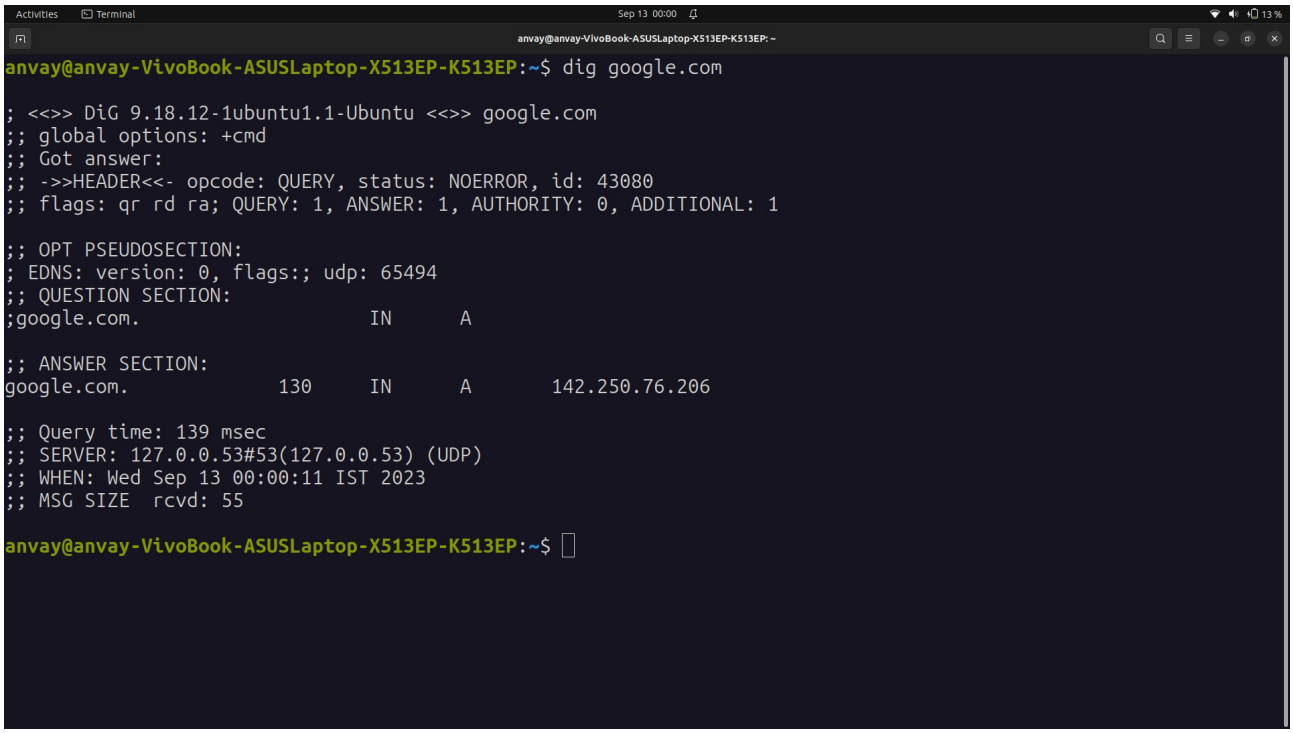
To obtain the IP address associated with a domain name (e.g., google.com):



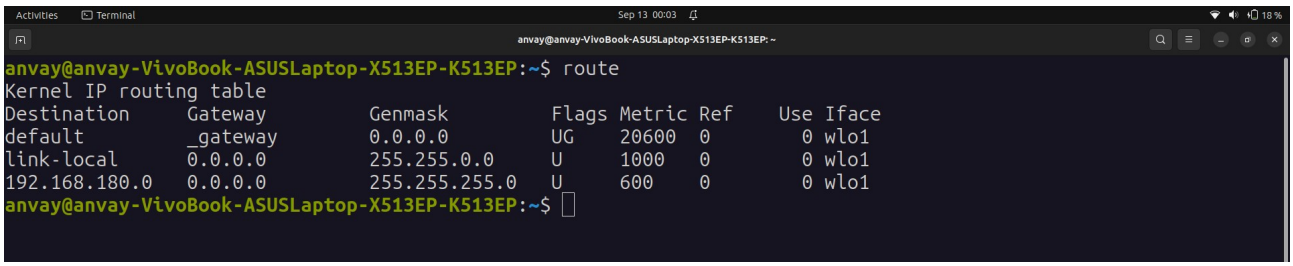
To obtain the IPv6 address (AAAA record) for a domain (e.g., ipv6.google.com):

8. dig

DESCRIPTION:
The dig command (short for Domain Information Groper) is a powerful and flexible command-line tool for querying Domain Name System (DNS) servers. It is commonly used on Unix-like operating systems, including Ubuntu, to retrieve various DNS-related information, such as IP addresses associated with domain names, DNS record types, and DNS server configurations.



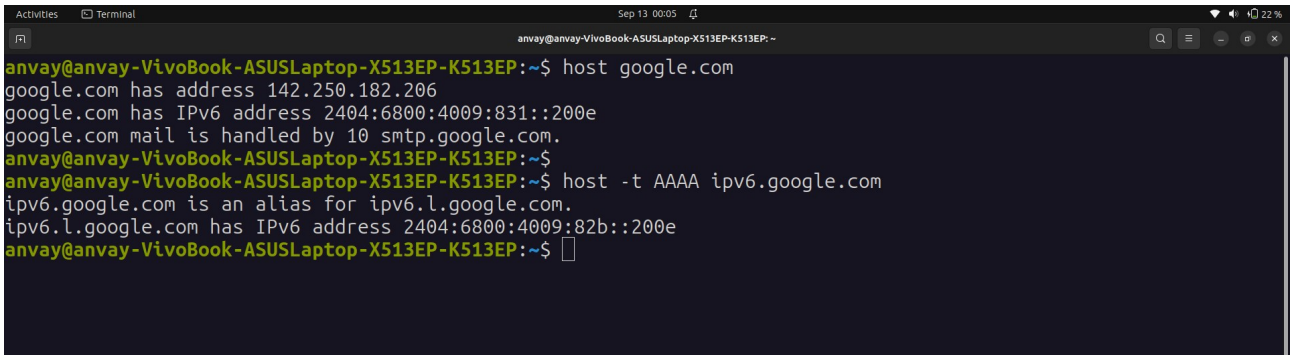
9. route
DESCRIPTION:
The `route` command in Linux is used to view and manipulate the kernel's IP routing table. It allows you to examine the routing table, add or delete routes, and make changes to the network configuration. This command is particularly useful for configuring static routes and diagnosing network-related issues.



10. host

DESCRIPTION:

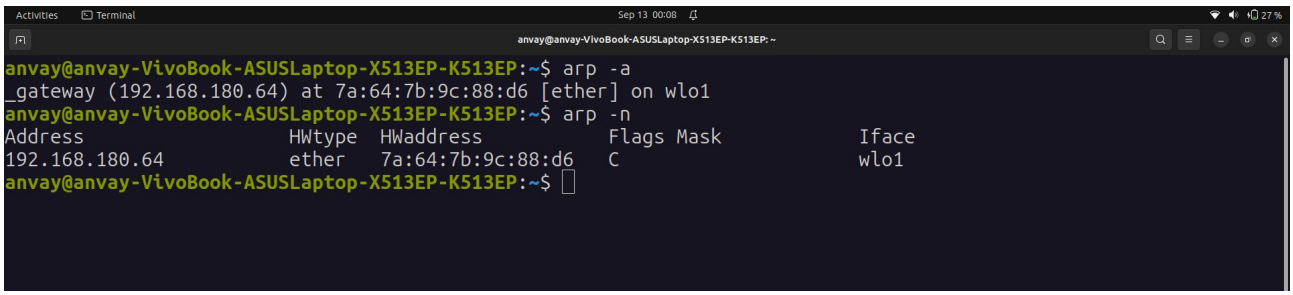
The `host` command in Linux is a DNS lookup utility used to query Domain Name System (DNS) servers to obtain information about domain names and IP addresses. It is primarily used to translate human-readable domain names into their corresponding IP addresses or vice versa. The `host` command is a simple and straightforward tool for DNS queries.



11. arp

DESCRIPTION:

The `arp` command in Linux is used to view and manipulate the Address Resolution Protocol (ARP) cache, which is a crucial part of how network devices map IP addresses to their corresponding physical MAC (Media Access Control) addresses on a local area network (LAN). ARP is essential for communication within a network, and the `arp` command allows you to inspect and manage the ARP cache on a Linux system



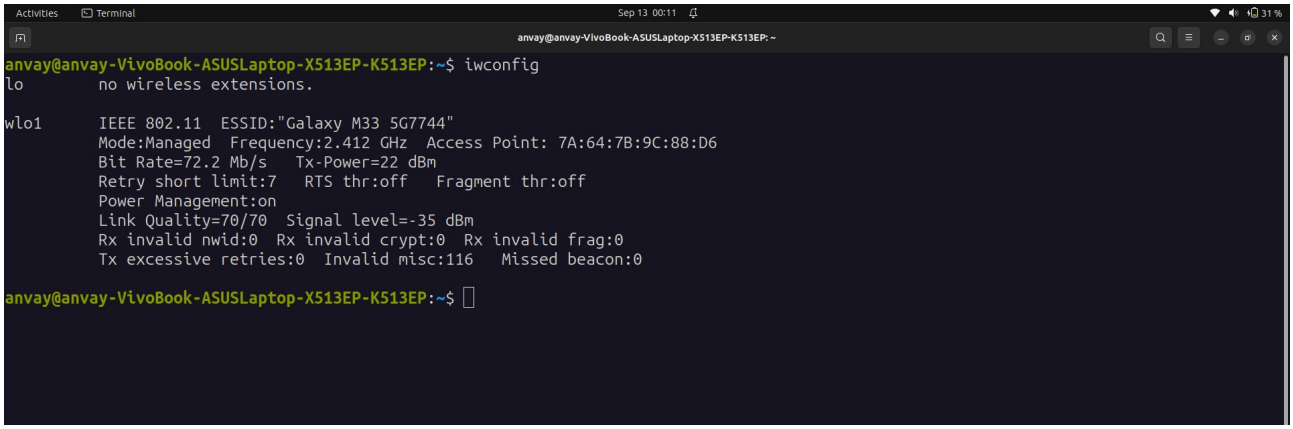
12. iwconfig

DESCRIPTION:

The iwconfig command in Linux is used to configure and display information about wireless

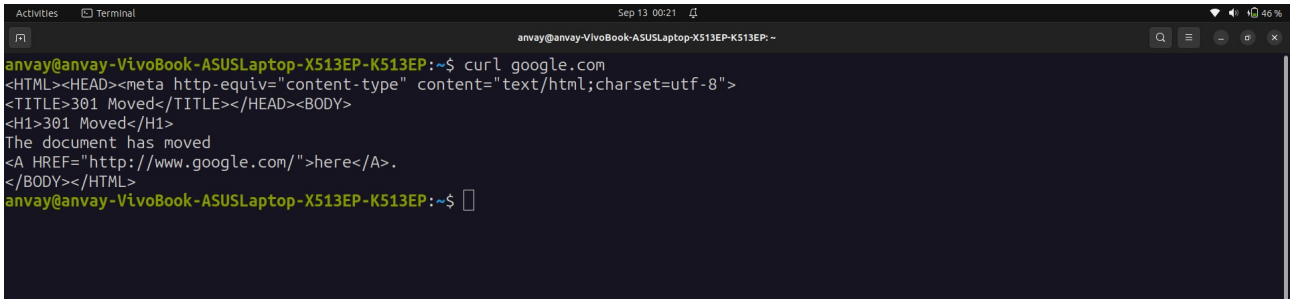
network interfaces. It is a part of the Wireless Tools package (wireless-tools), which is commonly installed on Linux systems with wireless network capabilities. iwconfig allows you to view information about your wireless network interface, configure wireless settings, and more.

Options :
-a: Display all information, including hidden interfaces.
-s: Show a short output with essential information



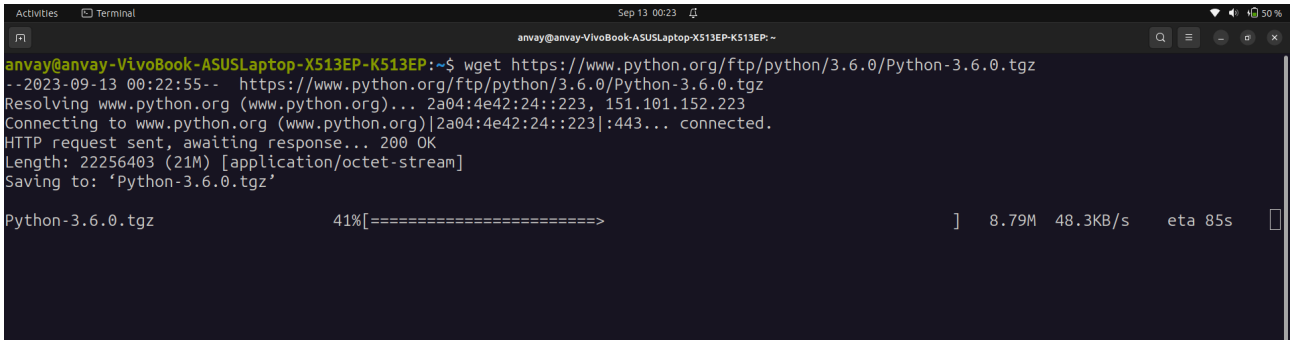
13. curl
DESCRIPTION:
The `curl` command in Linux is a versatile and powerful tool for making network requests to retrieve or send data to a remote server or web resource using various protocols. `curl` is commonly used for tasks such as downloading files, testing API endpoints, or interacting with web services.

It supports these protocols: DICT, FILE, FTP, FTPS, GOPHER, GOPHERS, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET, TFTP, WS and WSS. The command is designed to work without user interaction.



14. wget
DESCRIPTION:
The wget command is a versatile command-line utility used for downloading files from the internet. It supports various protocols, including HTTP, HTTPS, FTP, FTPS, and more. wget is available on most Unix-like operating systems, including Ubuntu and other Linux distributions. It is commonly

used for batch downloading, recursive fetching, and downloading files over the network.

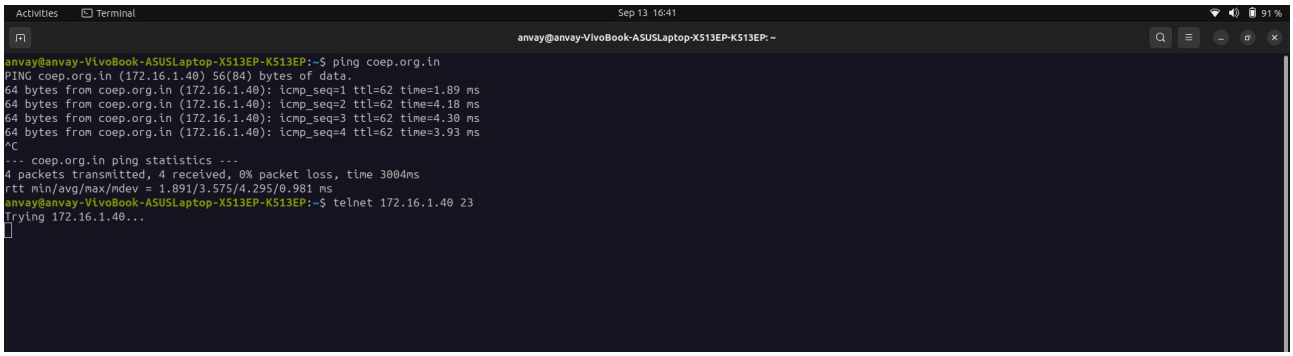


In above example, the .tgz package for python3.6 is being downloaded using wget.

15. telnet

DESCRIPTION:

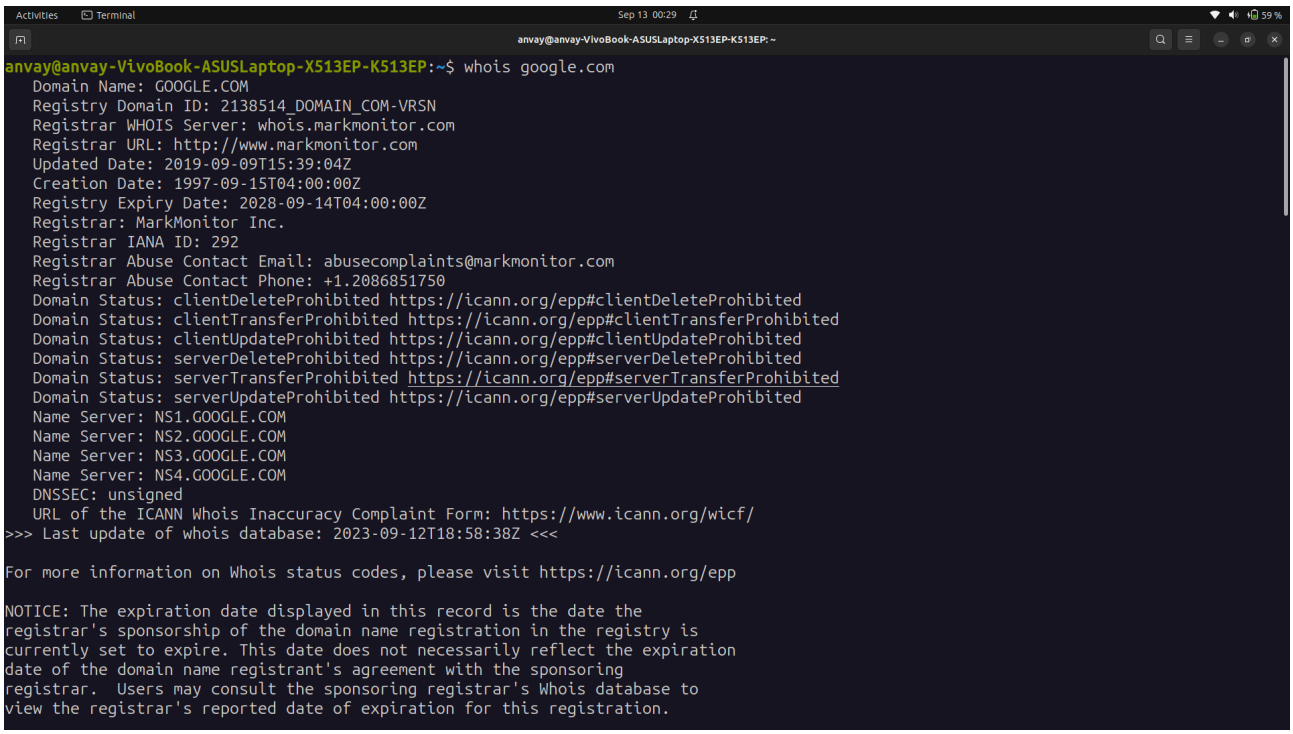
The telnet command is a command-line utility that allows you to establish a text-based network connection to a remote host or server over a network, typically using the Telnet protocol. It's available on most Unix-like operating systems, including Ubuntu and other Linux distributions. Telnet was historically used for remote access and administration of remote systems, but it's considered insecure for modern use due to its lack of encryption. Secure alternatives like SSH (Secure Shell) are recommended for remote access instead.



16. whois

DESCRIPTION:

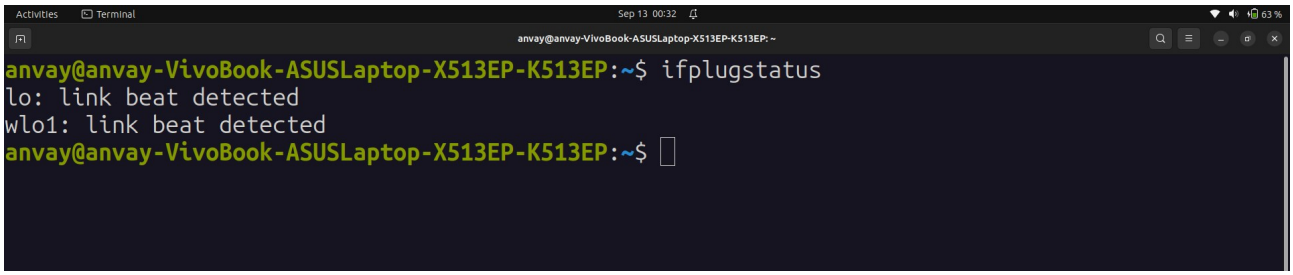
The `whois` command in Linux is a utility that allows you to retrieve information about domain names, IP addresses, and network resources from the Internet's domain name and address registration databases. It provides detailed information about the owner or administrator of a domain, its registration status, and other related information. The `whois` command is useful for checking domain name availability, obtaining contact information for a domain, and investigating network resources.



17. ifplugstatus

DESCRIPTION:

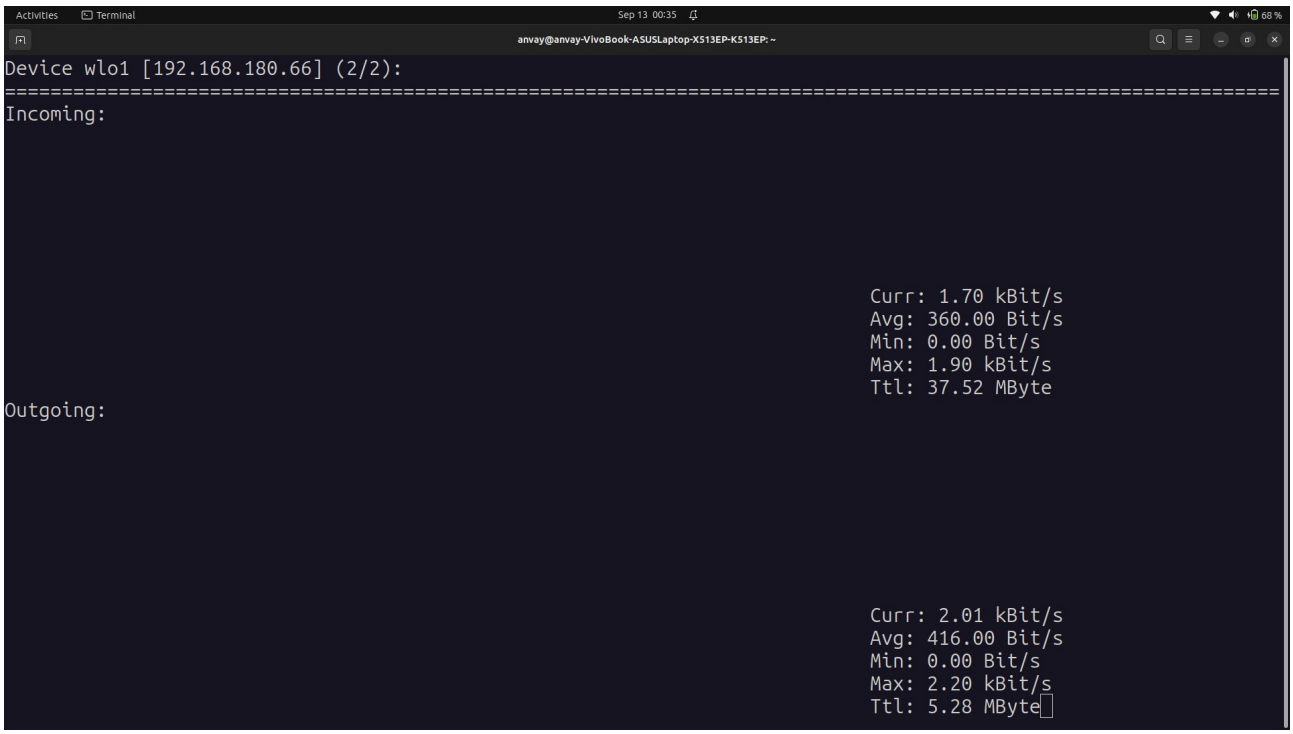
The `ifplugstatus` command is a utility used to check the status of network interfaces and determine whether a network cable is plugged into an Ethernet interface or not. This command is particularly useful for network administrators and users who need to monitor the physical status of Ethernet connections on a Linux system. It helps in diagnosing network connectivity issues and ensuring that network cables are properly connected.



18. nload

DESCRIPTION:

The `nload` command is a network monitoring tool available on Linux systems that provides a visual representation of network traffic and bandwidth usage in real-time. It is a command-line utility that allows you to view network statistics and monitor the incoming and outgoing network traffic on your system.



19.

20. mail

DESCRIPTION:

The `mail` command in Linux is a command-line utility that allows you to send and receive email messages from the command line. It provides a simple text-based interface for sending and reading emails. The `mail` command is often used for sending automated email notifications, scripting, and quick email tasks in a terminal environment.