UCS1512 Networks Lab

Exercise 1: Network Commands

**Commands**

# Command Name

Date: 18-08-2020

Name: Kshitij Sharma Register Number: 185001080

**tcpdump** - dump traffic on a network

# Syntax Description

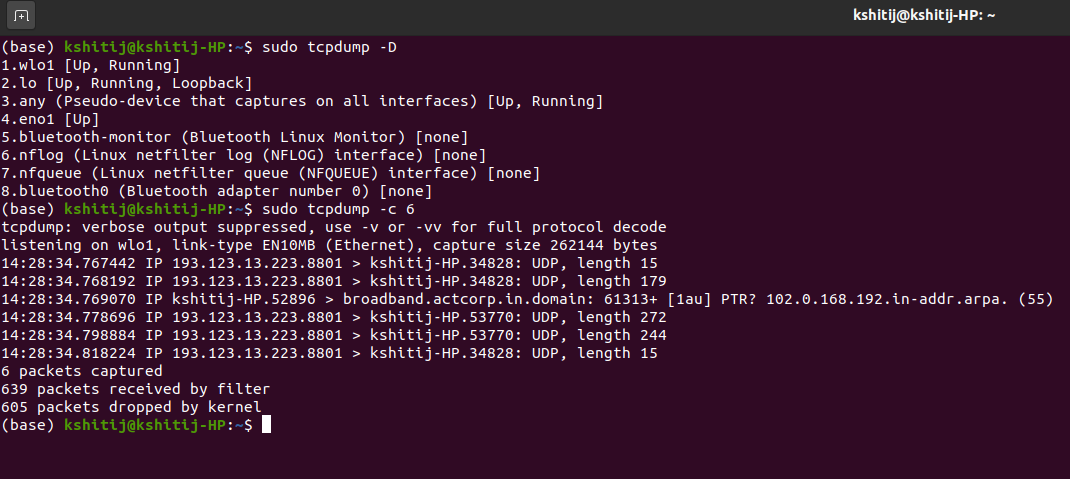
Tcpdump prints out a description of the contents of packets on a network interface that match the Boolean expression.The description is preceded by a timestamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. Tcpdump will, if not run with the -c flag, continue capturing packets until it is interrupted by a SIGINT signal (generated, for example, by typing your interrupt character, typically control-C) or a SIGTERM signal (typically generated with the kill(1) command). When tcpdump finishes capturing packets, it will report counts of: packets captured, packets received by filter and the number of packets that were dropped.

# Options

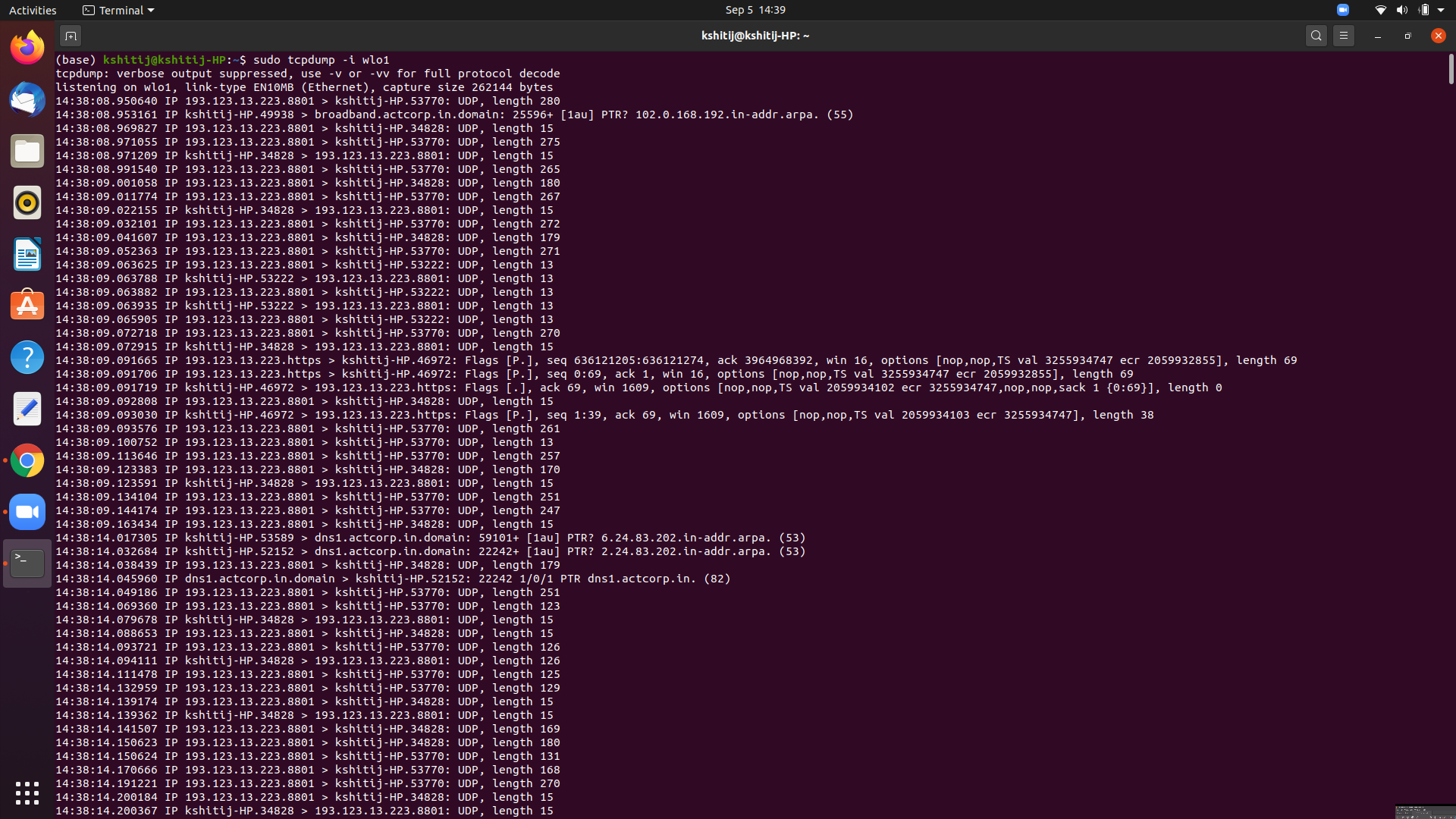
|  |  |
| --- | --- |
| -D  --list-interfaces | Print the list of the network interfaces available on the system and on which tcpdump can capture packets. |
| -i interface  --interface=int erface | Listen on interface. |
| -c count | Exit after receiving count packets. |

**Screenshots**

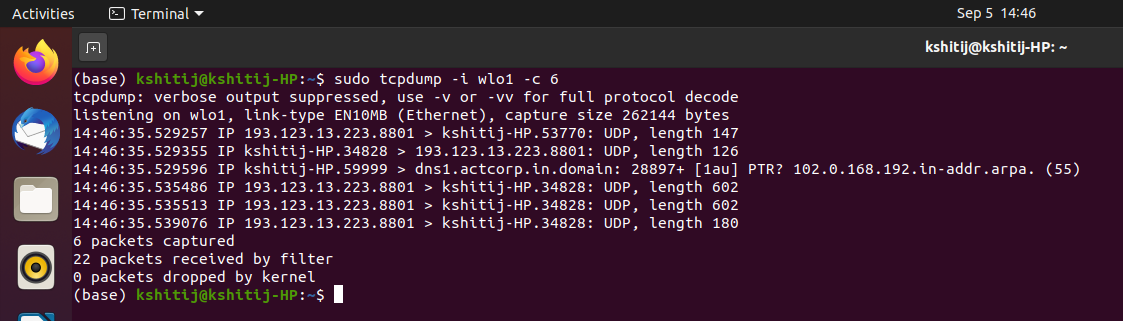
**tcpdump -D tcpdump -c 6**



**tcpdump -i wl01**



**tcpdump -i wlo1 -c6**



**Command Name**

**netstat** - Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

# Syntax Description

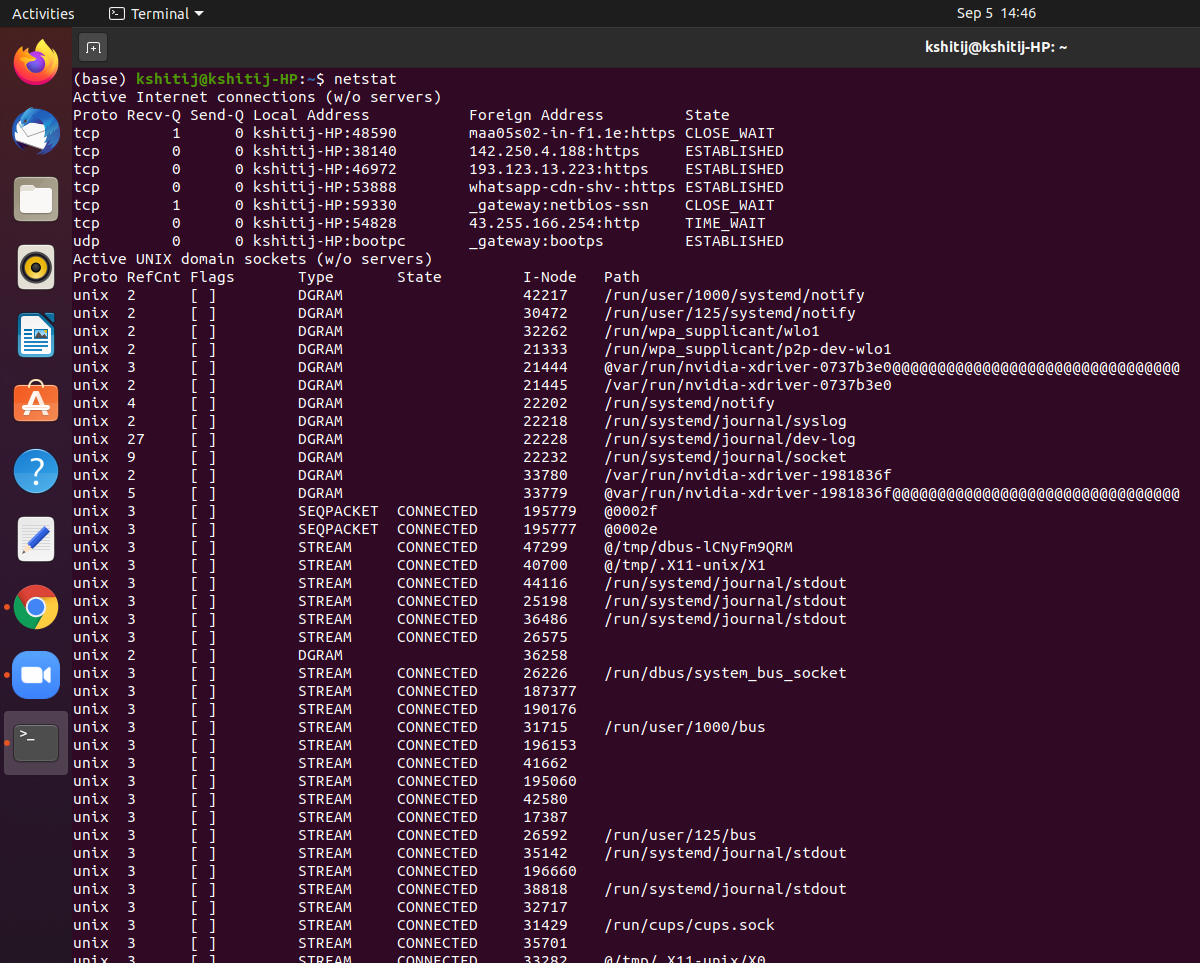
Netstat prints information about the Linux networking subsystem. The type of information printed is controlled by the first argument or option.

# Options

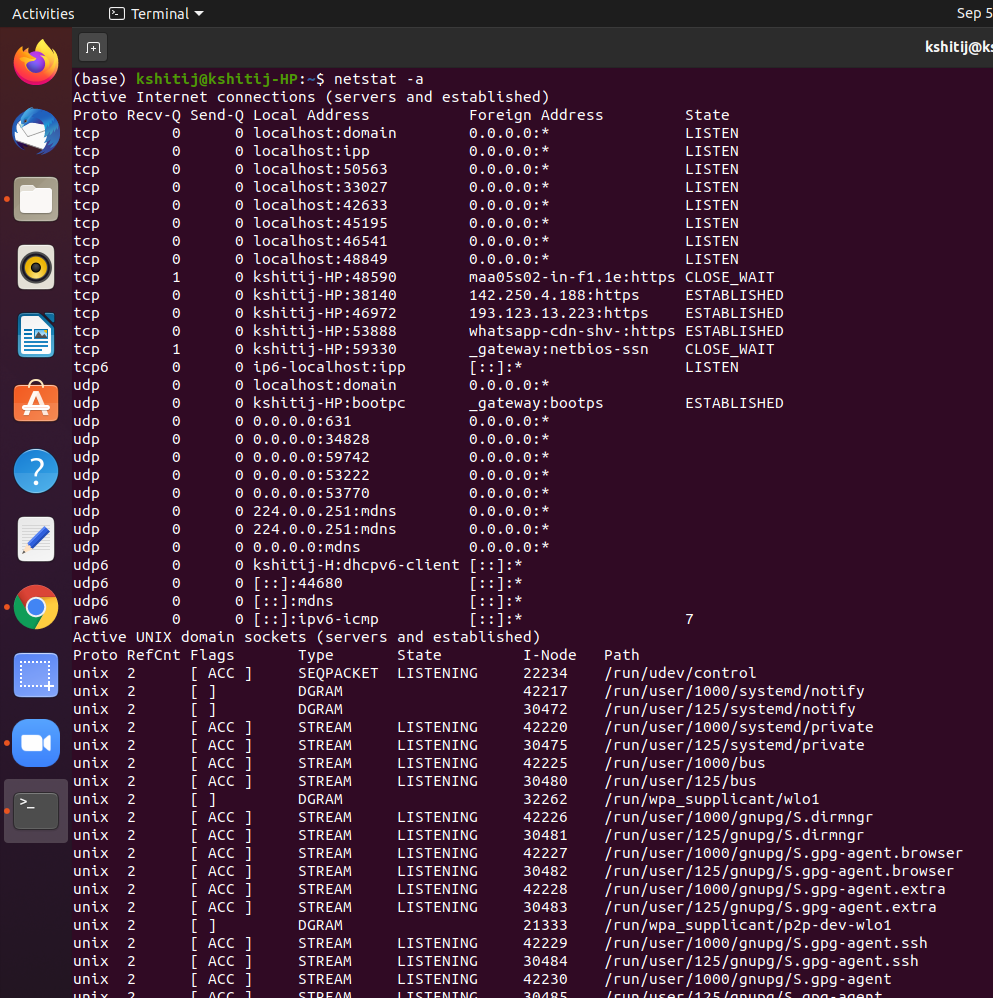
|  |  |
| --- | --- |
| (none) | By default, netstat displays a list of open sockets. If you don't specify any address families, then the active sockets of all configured address families will be printed. |
| -a, --all | Show both listening and non-listening (for TCP this means established connections) sockets. With the --interfaces option, show interfaces that are not marked. |
| --statistics , -s | Display summary statistics for each protocol. |
| -at | TCP internet connections. |
| -au | UDP internet connections. |
| -l, --listening | Show only listening sockets. (These are omitted by default.) |
| -lt | Listening TCP internet connections(servers). |
| -lu | Listening UDP internet connections(servers). |

**Screenshots**

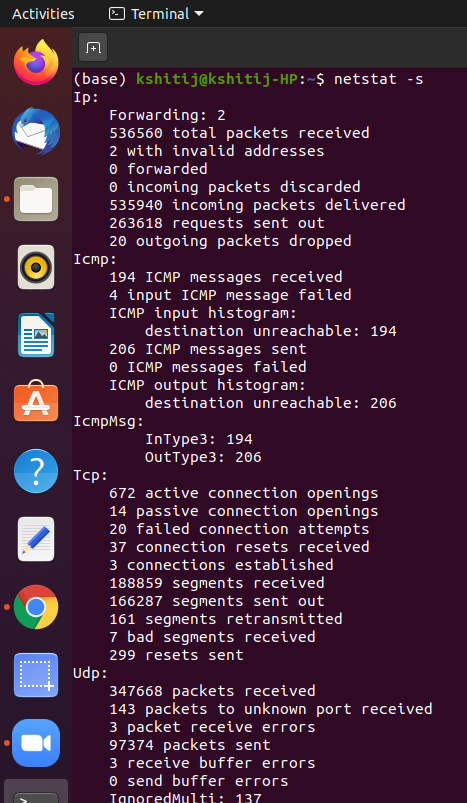
**netstat**



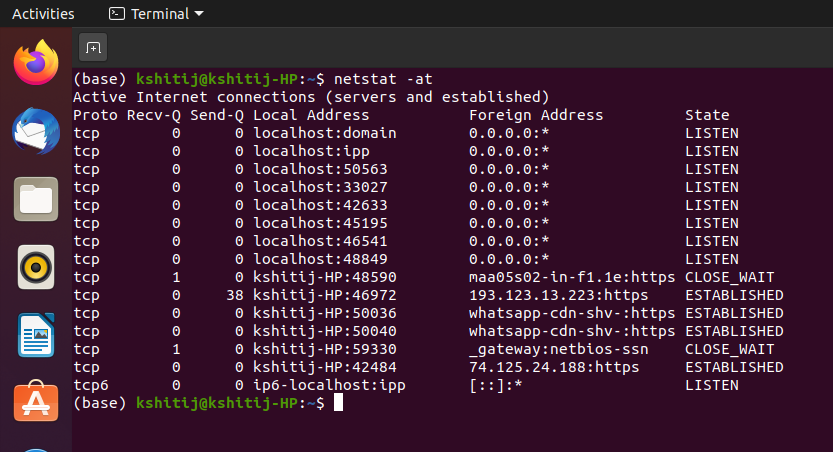
**netstat -a**



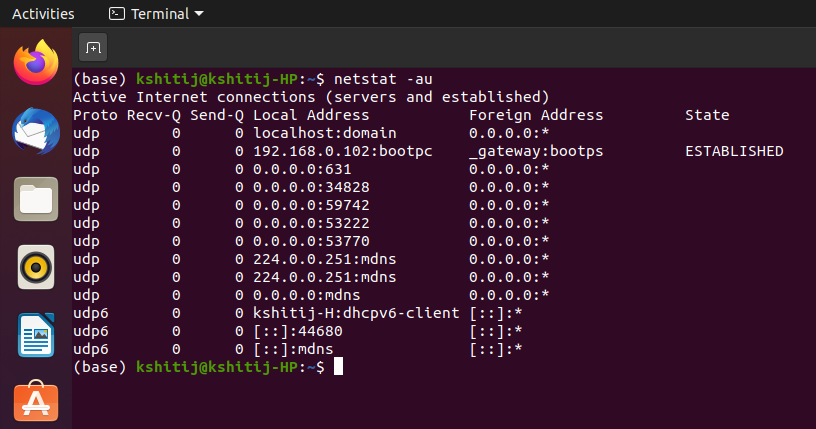
**netstat -s**



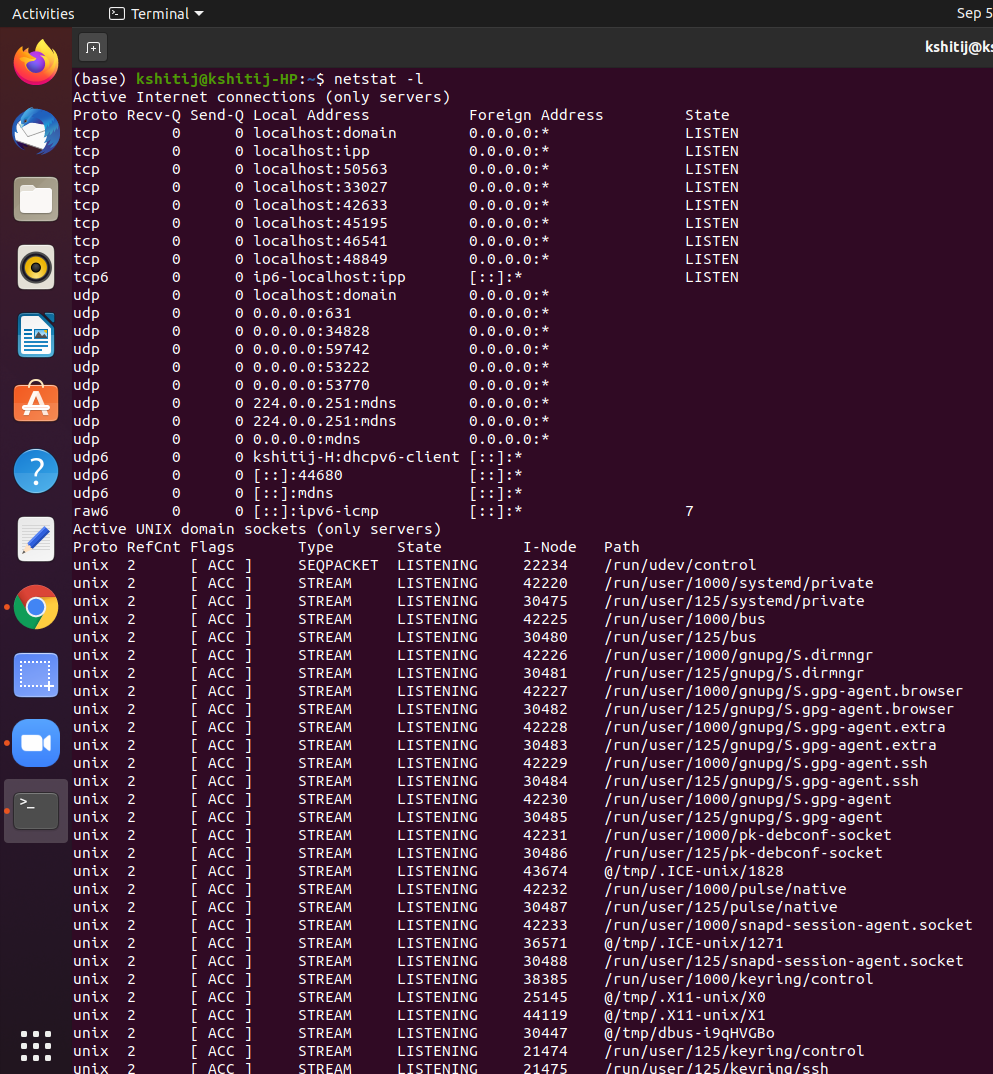
**netstat -at**



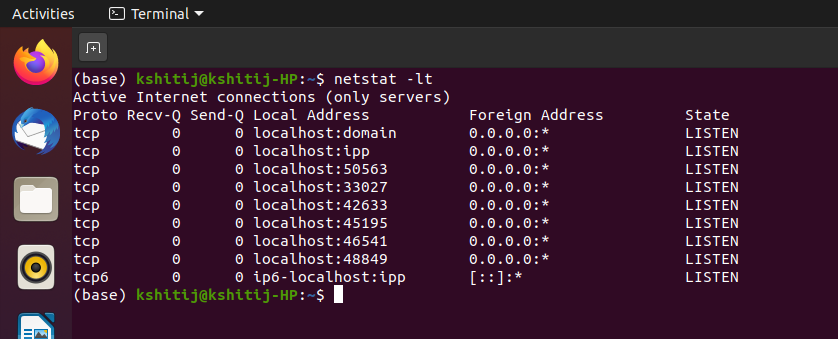
**netstat -au**



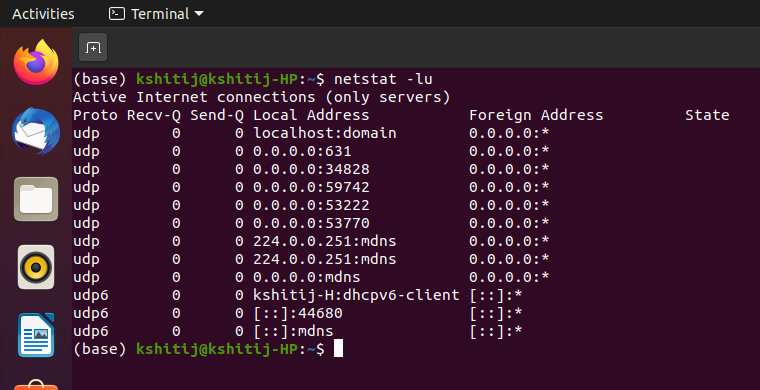
**netstat -l**



**netstat -lt**



**netstat -lu**



**Command Name**

**ifconfig** - configure a network interface

# Syntax Description

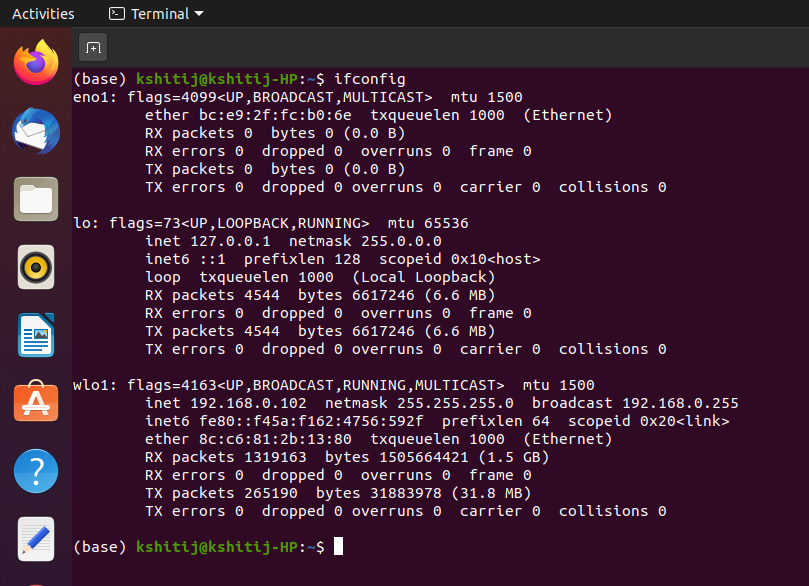
ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary; after that, it is usually only needed when debugging or when system tuning is needed.

# Options

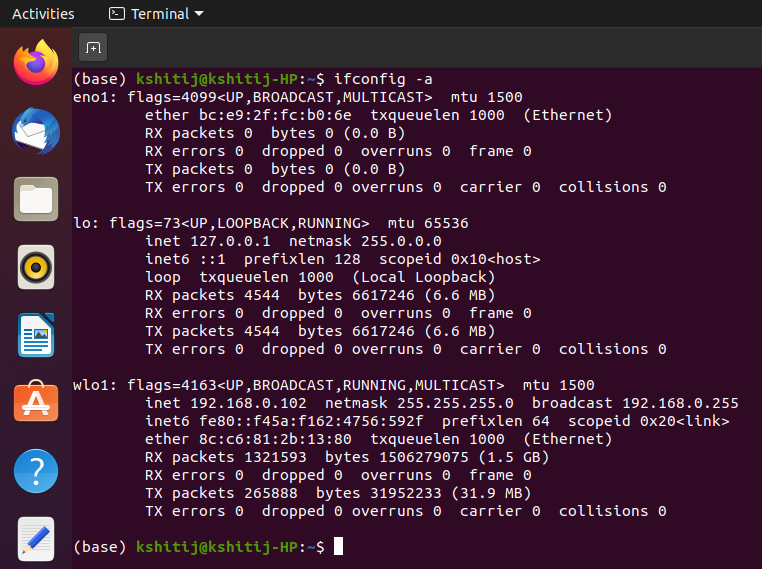
|  |  |
| --- | --- |
| (none) | If no arguments are given, ifconfig displays the status of the currently active interfaces. |
| -a | Display all interfaces which are currently available, even if down. |
| -s | Display a short list (like netstat -i). |
| interface | The name of the interface. |

**Screenshots**

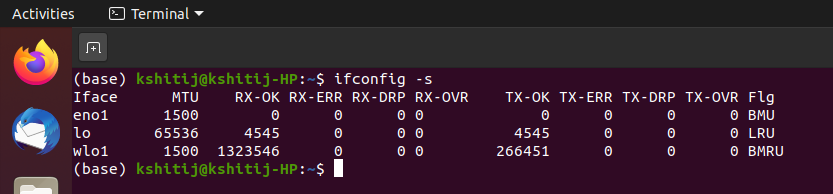
**Ifconfig**



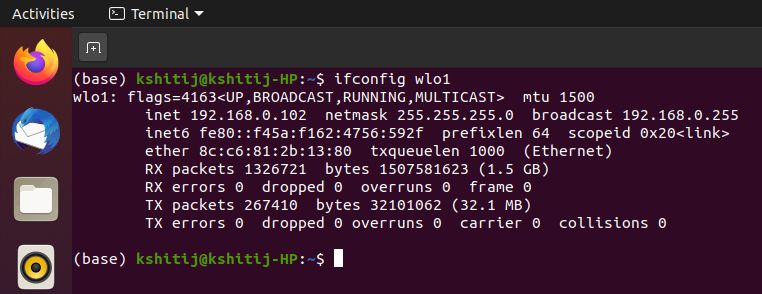
**ifconfig -a**



**ifconfig -s**



**ifconfig -wlo10**



**Command Name**

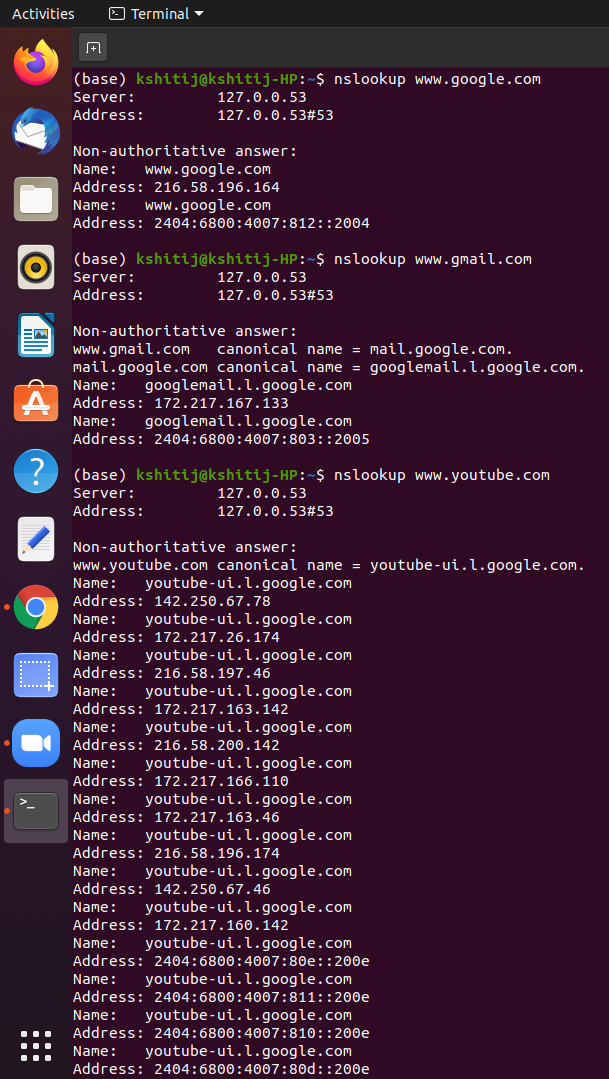
**nslookup** - query Internet name servers interactively

# Syntax Description

Nslookup is a program to query Internet domain name servers. Nslookup has two modes, Interactive mode and Non-interactive mode.

# Webpages & Screenshots

* [www.google.com](http://www.google.com/)
* [www.gmail.com](http://www.gmail.com/)
* [www.youtube.com](http://www.youtube.com/)



# Command Name

**traceroute** - print the route packets trace to network host

# Syntax Description

traceroute utilizes the IP protocol “time to live” field and attempts to elicit an ICMP TIME\_EXCEEDED response from each gateway along the path to some host.

The only mandatory parameter is the destination host name or IP number. The default probe datagram length is 40 bytes, but this may be increased by specifying a packet size (in bytes) after the destination host name.

# Webpages & Screenshots

* [www.google.com](http://www.google.com/)
* [www.gmail.com](http://www.gmail.com/)
* [www.youtube.com](http://www.youtube.com/)



# Command Name

**ping** - send ICMP ECHO\_REQUEST to network hosts

# Syntax Description

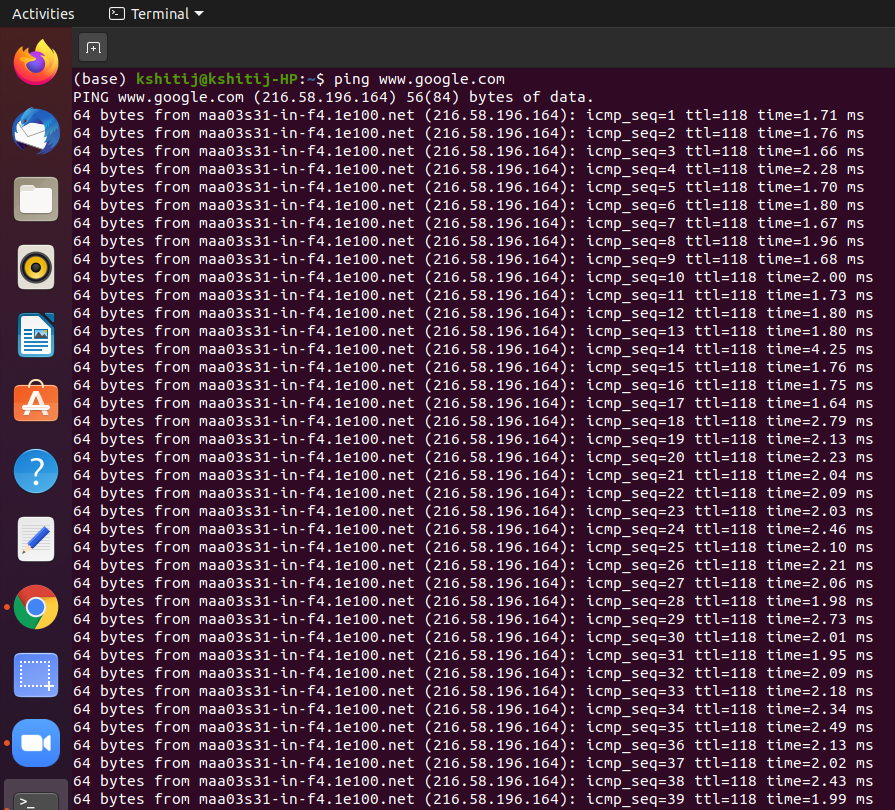
ping uses the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from a host or gateway. ECHO\_REQUEST datagrams (''pings'') have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of ''pad'' bytes used to fill out the packet.

# Webpages

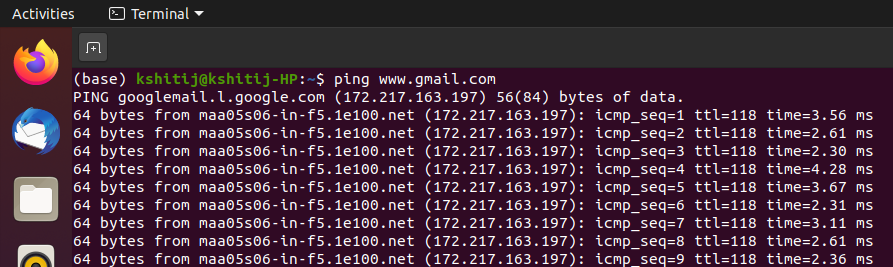
* [www.google.com](http://www.google.com/)
* [www.gmail.com](http://www.gmail.com/)
* [www.youtube.com](http://www.youtube.com/)

# Screenshots

ping [www.google.com](http://www.google.com/)



ping [www.gmail.com](http://www.google.com/)



ping [www.youtube.com](http://www.google.com/)

