Computer Networks Lab

Lab 2

Writer: Kalki Bhavsar

Date: August 23, 2020 Sunday

Prerequists - key terms

- **Network Interface**:

  A network interface is the point of interconnection between a computer and a private or public network. A network interface is generally a network interface card (NIC), but does not have to have a physical form (we can not see it, it is not a hardware!. Instead, the network interface can be implemented in software). For example, the loopback interface (127.0.0.1 for IPv4 and ::1 for IPv6) is not a physical device but a piece of software simulating a network interface.

- **Network interface card (NIC)**:

  A hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

  NIC allows both wired and wireless communications. NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP). NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

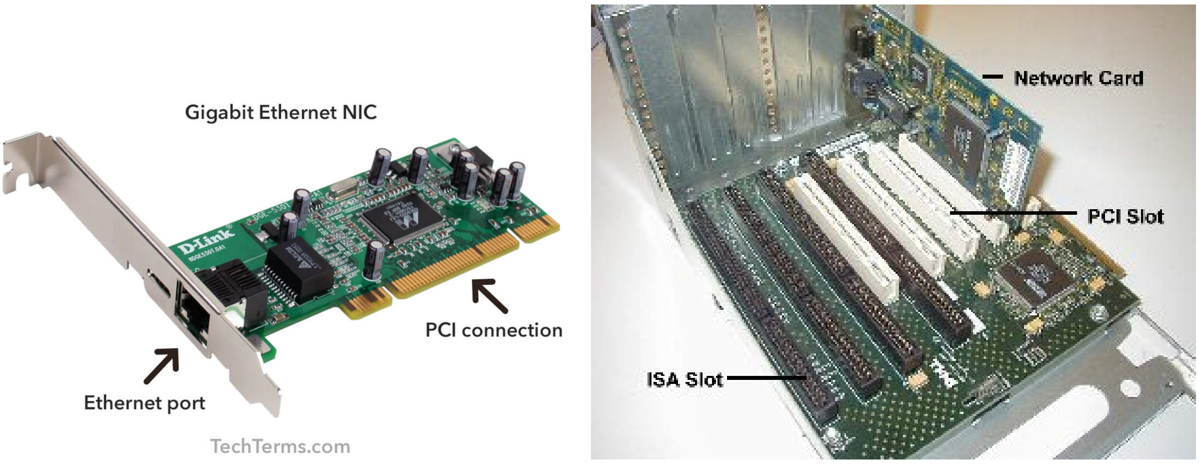


Figure 1: NIC with Ethernet port, PCI slot and ISA slot

  There are two kinds of NIC cards:

  - **Internal Network Cards**: The motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).
  - **External Network Cards**: In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

- **IP Address**: Computers in internet are connected with underwater cables or wirelessly. If you want to download a file from the internet, then your computer must have a unique address so that other computers in the WAN knows where to send the file i.e know the location of your computer. That address of your computer is called a IP address. IP address is just a string of numbers written in a certain format. Hence, an IP address stands for Internet Protocol address. Internet Protocol is a set of rules that makes computer work. You can watch a video in your computer/mobile because the device you are using has an IP address and application like Youtube or Netflix sends you the data related to that video at this IP address.

In short, IP address is used to identify computers on the Internet. When your computer or device sends a request, like a search on Google, it tags the request with your IP address. That way Google knows where to send the response.Your IP address is usually based on a real-world location. Google might use your IP address to guess where you are and give you local results. For example, Google could use your IP address to give you the weather forecast for the town you're in when you search for weather.

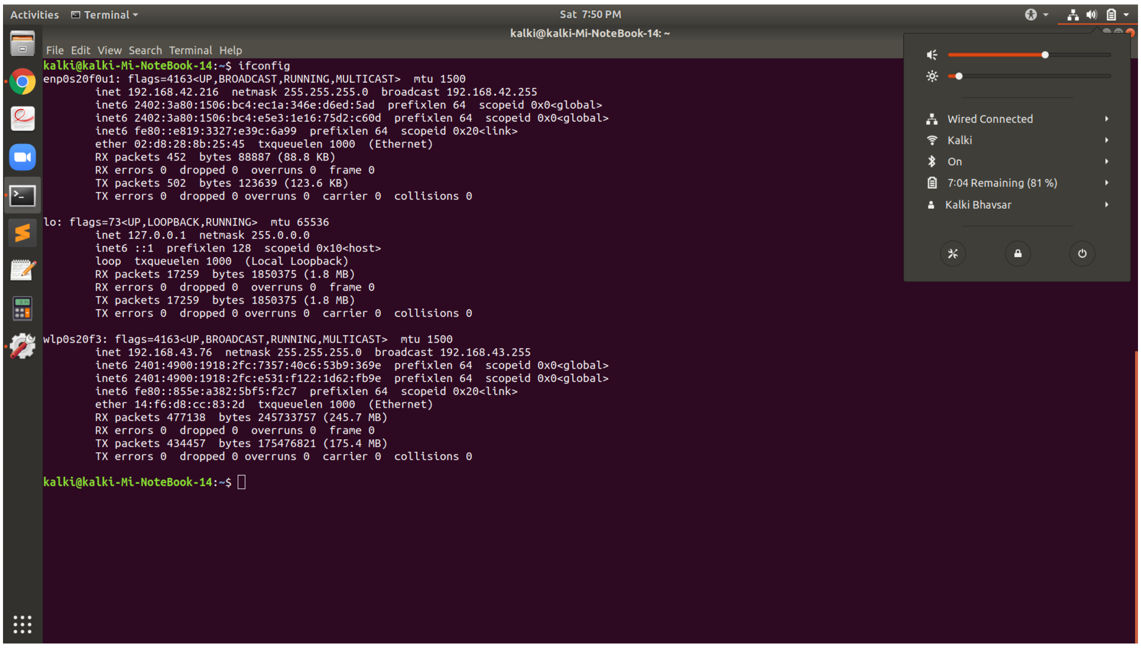
Now IP address are of two types.

- **IPV4**:
  - IPV4 format: **N.N.N.N** where **N** $\in [0, 255]$ **in decimal**
  - N $\in [00000000, 11111111]$ in binary. For each N, we require 8 bits or 1 byte.
  - For a IPV4 address, total memory required = 32 bits or 4 bytes
  - **IPV4 is a 32 bit IP address**
  - Total devices or total IPV4 address = 256^4 or 2^{32} = 4,294,967,296 devices or IPV4 addresses

  But total devices in current situation > 4,294,967,296
  Hence, IPV6 was invented.
- **IPV6**:
  - IPV6 format: **XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX**
    where **X** $\in$ **{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f} in hexa-decimal**
  - X $\in [0000, 1111]$. For each X, we require 4 bits or 1 nibble.
  - For a IPV6 address, total memory required = 128 bits or 16 bytes
  - **IPV6 is a 128 bit IP address**
  - Total devices or total IPV6 address = 16^{32} or 2^{128}
    = 340,282,366,920,938,463,463,374,607,431,768,211,456 devices or IPV6 addresses

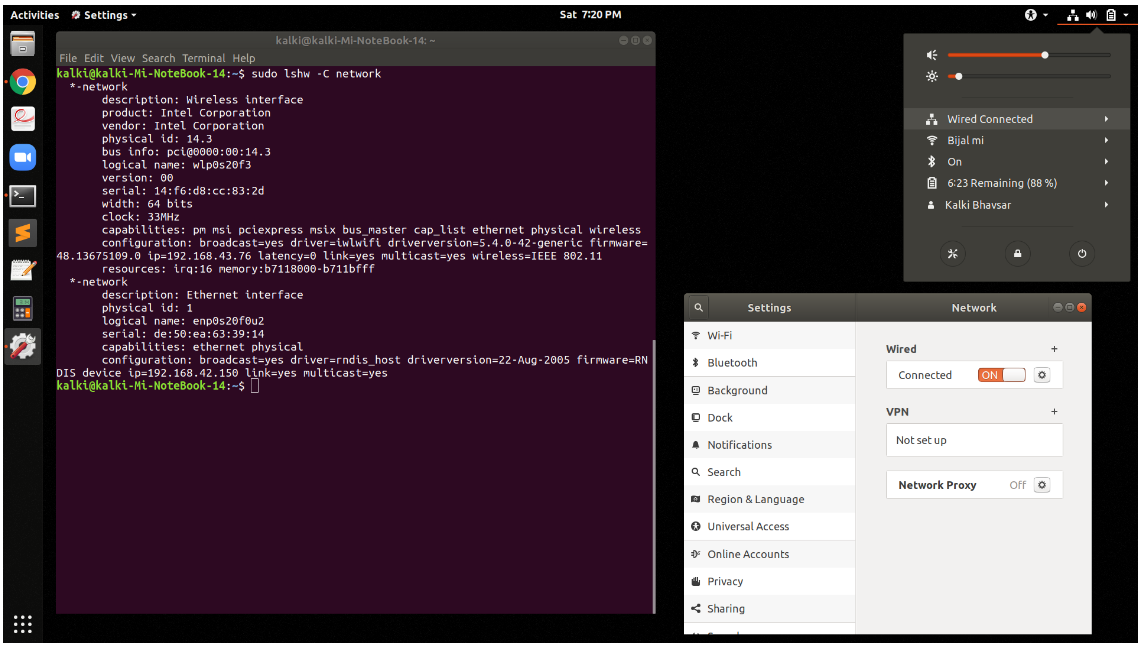
1 ipconfig

- **ipconfig (internet protocol configuration)**: a console application in Microsoft Windows that displays all current TCP/IP network configuration values and can modify Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.
- **ifconfig (short for interface configuration):** a system administration utility in Unix-like operating systems to configure, control, and query TCP/IP network interface parameters from a command line interface (CLI) or in system configuration scripts.The ifconfig command is used to get the information of active network-interfaces in a Unix-like operating system such as Linux, whereas ipconfig is used in the Windows OS.



```
kalki@kalki-Mi-NoteBook-14:~$ ifconfig
enp0s20f0u1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.216  netmask 255.255.255.0  broadcast 192.168.42.255
        inet6 2402:3a80:1506:bc4:ec1a:346e:d6ed:5ad  prefixlen 64  scopeid 0x0<global>
        inet6 2402:3a80:1506:bc4:e5e3:1e16:75d2:c60d  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::e819:3327:e39c:6a99  prefixlen 64  scopeid 0x20<link>
        ether 02:d8:28:8b:25:45  txqueuelen 1000  (Ethernet)
        RX packets 452  bytes 88887 (88.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 502  bytes 123639 (123.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 17259  bytes 1850375 (1.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17259  bytes 1850375 (1.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.76  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2401:4900:1918:2fc:7357:40c6:53b9:369e  prefixlen 64  scopeid 0x0<global>
        inet6 2401:4900:1918:2fc:e531:f122:1d62:fb9e  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::855e:a382:5bf5:f2c7  prefixlen 64  scopeid 0x20<link>
        ether 14:f6:d8:cc:83:2d  txqueuelen 1000  (Ethernet)
        RX packets 477138  bytes 245733757 (245.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 434457  bytes 175476821 (175.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kalki@kalki-Mi-NoteBook-14:~$ 
```

Figure 2: ifconfig: list all active network-interfaces

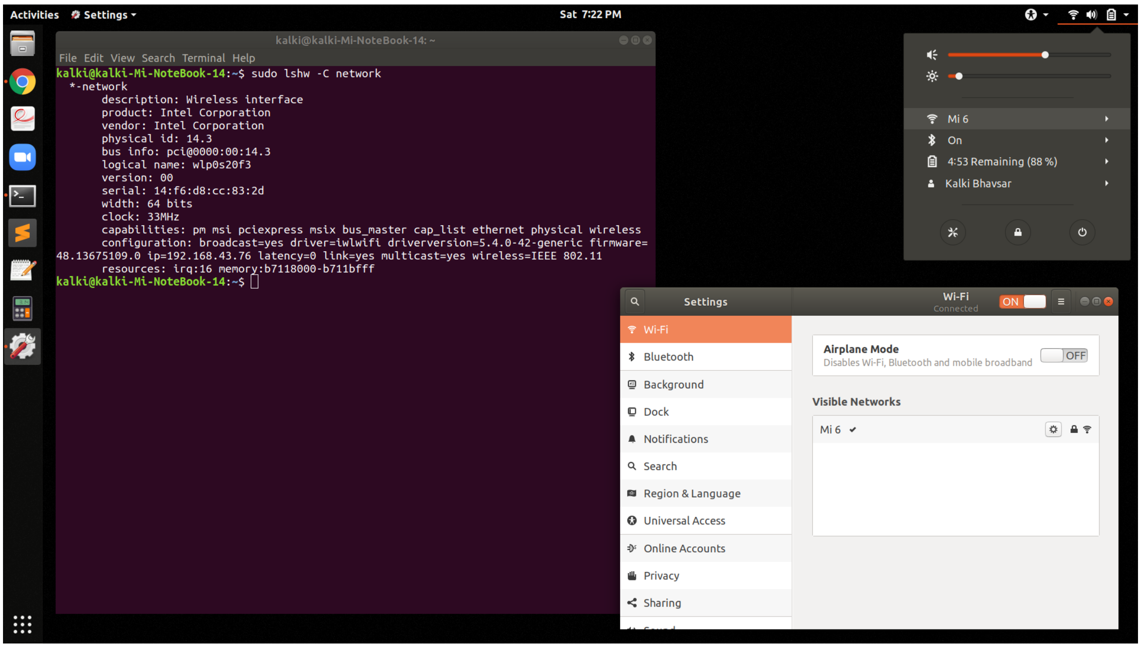


```
kalki@kalki-Mi-NoteBook-14:~$ sudo lshw -C network
  *-network
       description: Wireless interface
       product: Intel Corporation
       vendor: Intel Corporation
       physical id: 14.3
       bus info: pci@0000:00:14.3
       logical name: wlp0s20f3
       version: 00
       serial: 14:f6:d8:cc:83:2d
       width: 64 bits
       clock: 33MHz
       capabilities: pm msi pciexpress msix bus_master cap_list ethernet physical wireless
       configuration: broadcast=yes driver=iwlwifi driverversion=5.4.0-42-generic firmware=
48.13675109.0 ip=192.168.43.76 latency=0 link=yes multicast=yes wireless=IEEE 802.11
       resources: irq:16 memory:b7118000-b711bfff
  *-network
       description: Ethernet interface
       physical id: 1
       logical name: enp0s20f0u2
       serial: de:50:ea:63:39:14
       capabilities: ethernet physical
       configuration: broadcast=yes driver=rndis_host driverversion=22-Aug-2005 firmware=RN
DIS device ip=192.168.42.150 link=yes multicast=yes
kalki@kalki-Mi-NoteBook-14:~$ 
```

Wired Connected
Bijal mi
On
6:23 Remaining (88 %)
Kalki Bhavsar

Network
Wired: Connected ON
VPN: Not set up
Network Proxy: Off

Figure 3: Wired Connection-enp0 as well as Wireless Connection-wlp0



```
kalki@kalki-Mi-NoteBook-14:~$ sudo lshw -C network
  *-network
       description: Wireless interface
       product: Intel Corporation
       vendor: Intel Corporation
       physical id: 14.3
       bus info: pci@0000:00:14.3
       logical name: wlp0s20f3
       version: 00
       serial: 14:f6:d8:cc:83:2d
       width: 64 bits
       clock: 33MHz
       capabilities: pm msi pciexpress msix bus_master cap_list ethernet physical wireless
       configuration: broadcast=yes driver=iwlwifi driverversion=5.4.0-42-generic firmware=
48.13675109.0 ip=192.168.43.76 latency=0 link=yes multicast=yes wireless=IEEE 802.11
       resources: irq:16 memory:b7118000-b711bfff
kalki@kalki-Mi-NoteBook-14:~$ 
```

Mi 6
On
4:53 Remaining (88 %)
Kalki Bhavsar

Wi-Fi Connected ON
Airplane Mode OFF
Disables Wi-Fi, Bluetooth and mobile broadband
Visible Networks
Mi 6 ✓

Figure 4: Only Wireless Connection-wlp0

2 ping

- Ping comes from a term used in sonar technology that sends out pulses of sound, and then listens for the echo to return.

- On a computer network, a ping tool is built into most operating systems that works in much the same way. You issue the ping command along with a specific URL or IP address. Your computer sends several packets of information out to that device, and then waits for a response. When it gets the response, the ping tool shows you how long each packet took to make the round trip—or tells you there was no reply.

- PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message "PING" and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. Ping uses ICMP(Internet Control Message Protocol) to send an ICMP echo message to the specified host if that host is available then it sends ICMP reply message.

- That response shows the URL you're pinging, the IP address associated with that URL, and the size of the packets being sent on the first line. The next four lines show the replies from each individual packet, including the time (in milliseconds) it took for the response and the time-to-live (TTL) of the packet, which is the amount of time that must pass before the packet is discarded. At the bottom, you'll see a summary that shows how many packets were sent and received, as well as the minimum, maximum, and average response time.

  Uses:

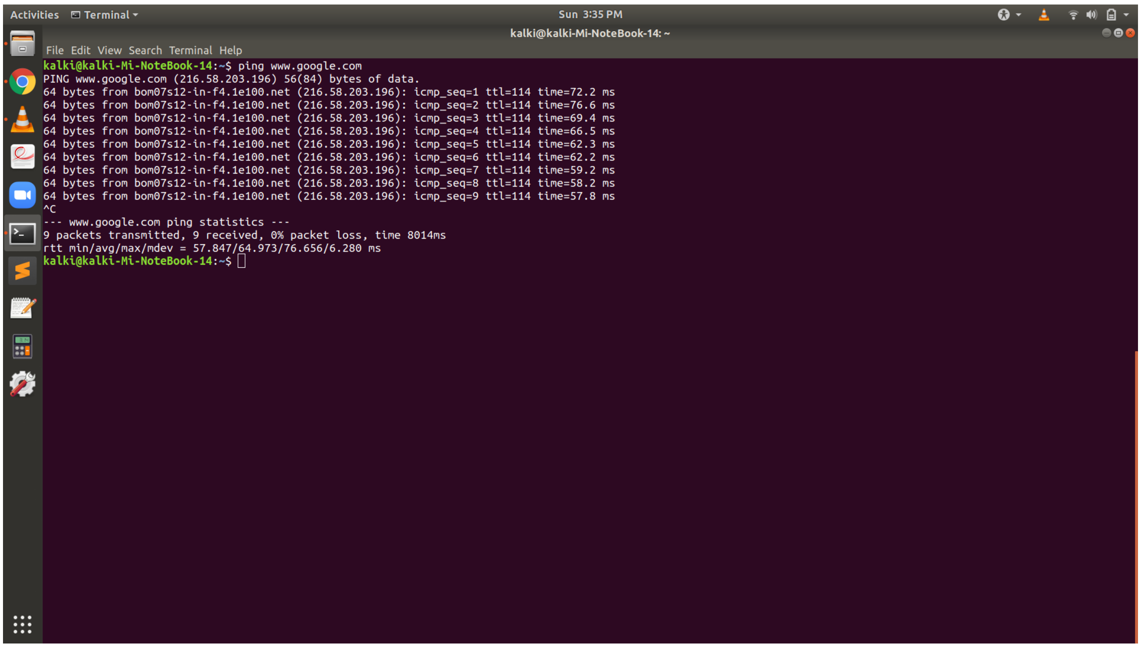
- Test whether your computer can reach another device—like your router—on your local network, or whether it can reach a device on the Internet. This can help you determine if a network problem is somewhere on your local network, or somewhere beyond.

- The time it takes packets to return to you can help you identify a slow connection, or if you're experiencing packet loss.

- If you want know the IP address for a particular URL, you can ping the URL.

- Ping a URL (like www.howtogeek.com) or IP address to see if you can reach an internet destination. If you get a successful response, you know that all the networking devices between you and that destination are working, including the network adapter in your computer, your router, and whatever devices exist on the internet between your router and the destination.

- Ping your router to see if you can reach it. If you can't successfully ping an internet location, you can then try pinging your router. A successful response lets you know that your local network is working okay, and that the problem reaching the internet location is somewhere out of your control.



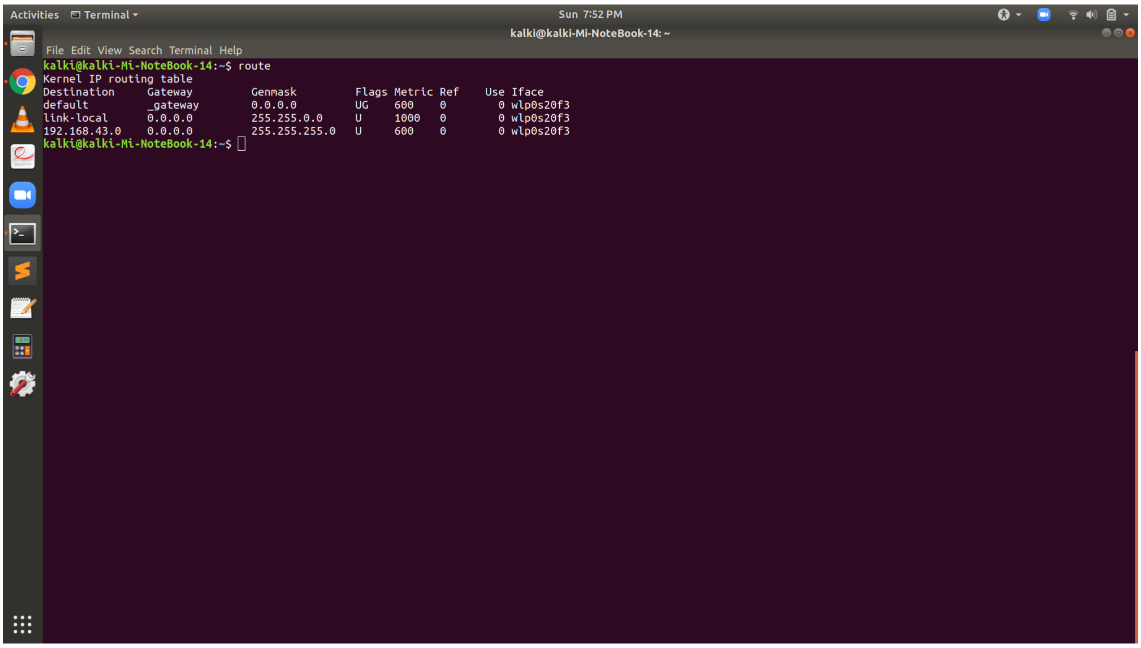
Activities
Terminal
Sun 3:35 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ ping www.google.com
PING www.google.com (216.58.203.196) 56(84) bytes of data.
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=1 ttl=114 time=72.2 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=2 ttl=114 time=76.6 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=3 ttl=114 time=69.4 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=4 ttl=114 time=66.5 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=5 ttl=114 time=62.3 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=6 ttl=114 time=62.2 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=7 ttl=114 time=59.2 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=8 ttl=114 time=58.2 ms
64 bytes from bom07s12-in-f4.1e100.net (216.58.203.196): icmp_seq=9 ttl=114 time=57.8 ms
^C
--- www.google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8014ms
rtt min/avg/max/mdev = 57.847/64.973/76.656/6.280 ms
kalki@kalki-Mi-NoteBook-14:~$ 
```

Figure 5: ping command: ping to www.google.com

3 route

- Intallation: $sudo apt-get install net-tools
- route command in Linux is used when you want to work with the IP/kernel routing table.
- It is mainly used to set up static routes to specific hosts or networks via an interface.
- It is used for showing or update the IP/kernel routing table.



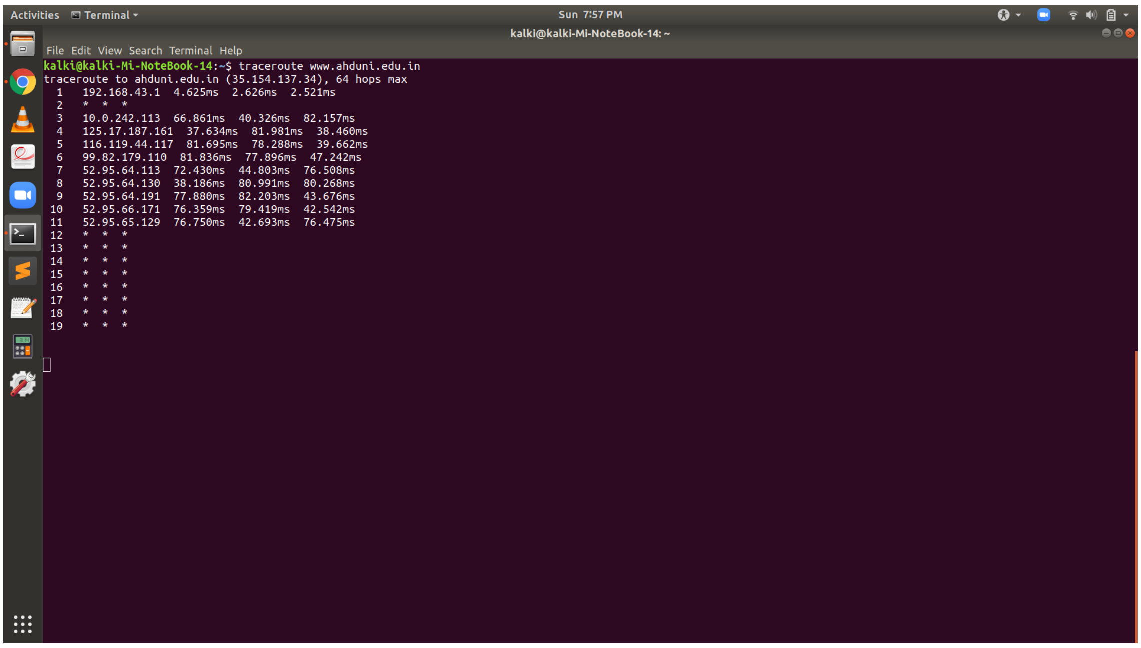
Activities
Terminal
Sun 7:52 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp0s20f3
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp0s20f3
kalki@kalki-Mi-NoteBook-14:~$ 
```

Figure 6: route

4 traceroute

- When packets are sent across the internet, they must hop from network to network.
- The traceroute command traces the route that packets takes to reach the host.
- It will show you how many hops it takes to reach the host and how long it took between each hop.
- This allows you to diagnose potential networking bottlenecks. (If the system working on a network is delivering a higher volume of data than what is supported by the existing capacity of the network, then a network bottleneck will occur. A common computing bottleneck culprit is network data interruption caused by microprocessor circuitry or TCP/IP).
- The example below shows the traceroute command output from your local PC to Google server.

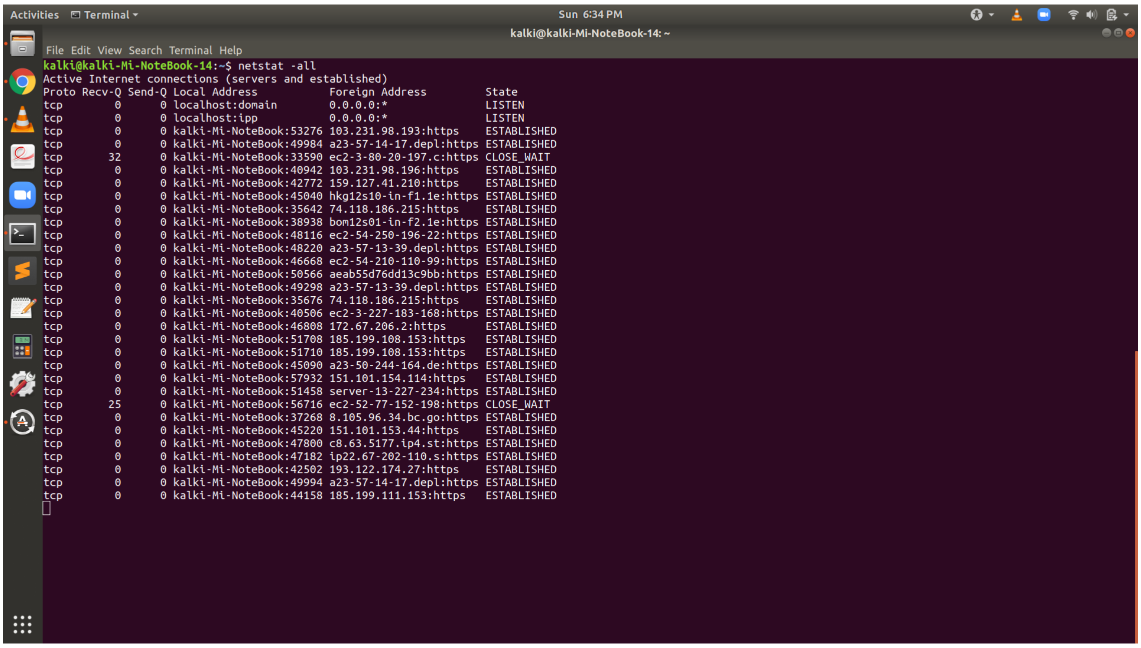

Activities
Terminal
Sun 7:57 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ traceroute www.ahduni.edu.in
traceroute to ahduni.edu.in (35.154.137.34), 64 hops max
  1   192.168.43.1  4.625ms  2.626ms  2.521ms
  2   *  *  *
  3   10.0.242.113  66.861ms  40.326ms  82.157ms
  4   125.17.187.161  37.634ms  81.981ms  38.460ms
  5   116.119.44.117  81.695ms  78.288ms  39.662ms
  6   99.82.179.110  81.836ms  77.896ms  47.242ms
  7   52.95.64.113  72.430ms  44.803ms  76.508ms
  8   52.95.64.130  38.186ms  80.991ms  80.268ms
  9   52.95.64.191  77.880ms  82.203ms  43.676ms
 10   52.95.66.171  76.359ms  79.419ms  42.542ms
 11   52.95.65.129  76.750ms  42.693ms  76.475ms
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   *  *  *
```

Figure 7: traceroute command: ping to www.ahduni.edu.in

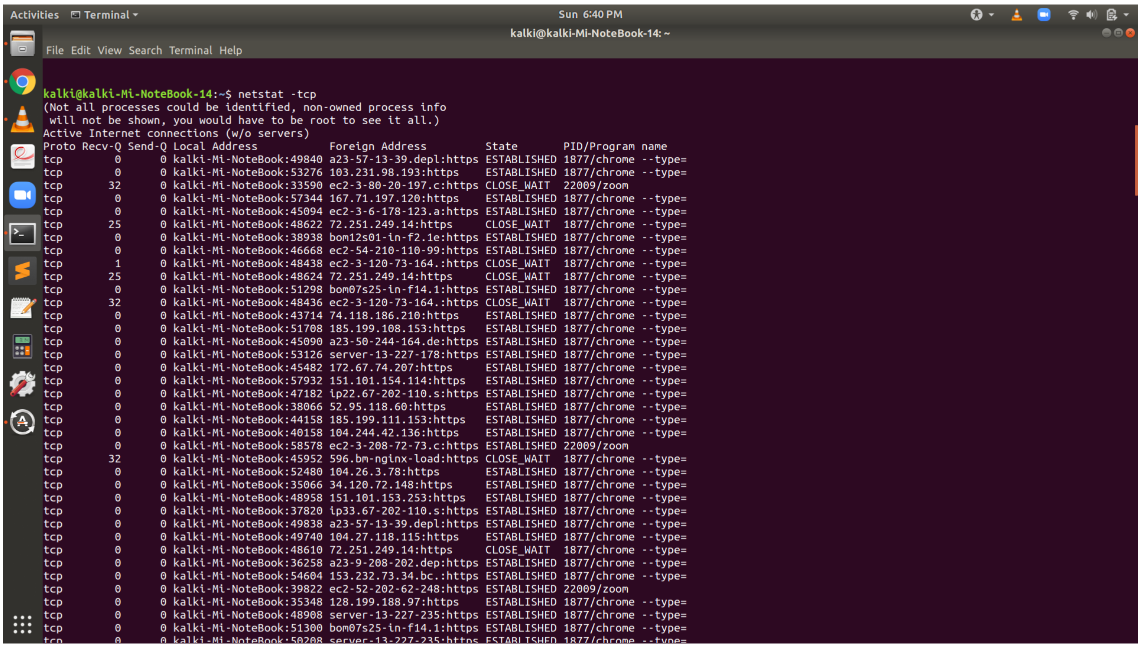
5 netstat

- Netstat is a command line utility that can be utilized to list out all the network (socket) connections on a method comparable to network connections, routing tables, interface records, masquerade connections, multicast memberships etc.
- **Usage:**It can be used to troubleshoot network-related issues and verify connection statistics.


Activities
Terminal
Sun 6:34 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

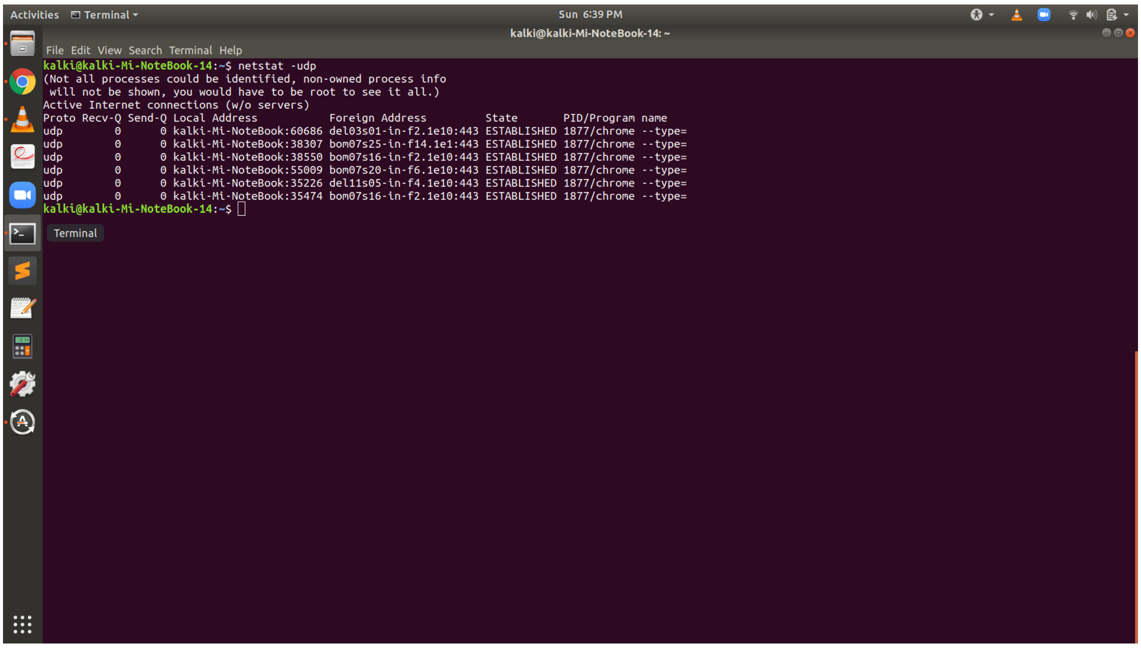
```
kalki@kalki-Mi-NoteBook-14:~$ netstat -all
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 kalki-Mi-NoteBook:53276 103.231.98.193:https    ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:49984 a23-57-14-17.depl:https ESTABLISHED
tcp       32      0 kalki-Mi-NoteBook:33590 ec2-3-80-20-197.c:https CLOSE_WAIT
tcp        0      0 kalki-Mi-NoteBook:40942 103.231.98.196:https    ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:42772 159.127.41.210:https    ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:45040 hkg12s10-in-f1.1e:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:35642 74.118.186.215:https    ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:38938 bom12s01-in-f2.1e:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:48116 ec2-54-250-196-22:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:48220 a23-57-13-39.depl:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:46668 ec2-54-210-110-99:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:50566 aeab55d76dd13c9bb:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:49298 a23-57-13-39.depl:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:35676 74.118.186.215:https    ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:40506 ec2-3-227-183-168:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:46808 172.67.206.2:https      ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:51708 185.199.108.153:https   ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:51710 185.199.108.153:https   ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:45090 a23-50-244-164.de:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:57932 151.101.154.114:https   ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:51458 server-13-227-234:https ESTABLISHED
tcp       25      0 kalki-Mi-NoteBook:56716 ec2-52-77-152-198:https CLOSE_WAIT
tcp        0      0 kalki-Mi-NoteBook:37268 8.105.96.34.bc.go:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:45220 151.101.153.44:https    ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:47800 c8.63.5177.ip4.st:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:47182 ip22.67-202-110.s:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:42502 193.122.174.27:https    ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:49994 a23-57-14-17.depl:https ESTABLISHED
tcp        0      0 kalki-Mi-NoteBook:44158 185.199.111.153:https   ESTABLISHED
```

Figure 8: netstat -a: To show both listening and non-listening sockets.


Activities
Terminal
Sun 6:40 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ netstat -tcp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 kalki-Mi-NoteBook:49840 a23-57-13-39.depl:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:53276 103.231.98.193:https    ESTABLISHED 1877/chrome --type=
tcp       32      0 kalki-Mi-NoteBook:33590 ec2-3-80-20-197.c:https CLOSE_WAIT  22009/zoom
tcp        0      0 kalki-Mi-NoteBook:57344 167.71.197.120:https    ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:45094 ec2-3-6-178-123.a:https ESTABLISHED 1877/chrome --type=
tcp       25      0 kalki-Mi-NoteBook:48622 72.251.249.14:https     CLOSE_WAIT  1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:38938 bom12s01-in-f2.1e:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:46668 ec2-54-210-110-99:https ESTABLISHED 1877/chrome --type=
tcp        1      0 kalki-Mi-NoteBook:48438 ec2-3-120-73-164.:https CLOSE_WAIT  1877/chrome --type=
tcp       25      0 kalki-Mi-NoteBook:48624 72.251.249.14:https     CLOSE_WAIT  1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:51298 bom07s25-in-f14.1:https ESTABLISHED 1877/chrome --type=
tcp       32      0 kalki-Mi-NoteBook:48436 ec2-3-120-73-164.:https CLOSE_WAIT  1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:43714 74.118.186.210:https    ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:51708 185.199.108.153:https   ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:45090 a23-50-244-164.de:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:53126 server-13-227-178:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:45482 172.67.74.207:https     ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:57932 151.101.154.114:https   ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:47182 ip22.67-202-110.s:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:38066 52.95.118.60:https      ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:44158 185.199.111.153:https   ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:40158 104.244.42.136:https    ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:58578 ec2-3-208-72-73.c:https ESTABLISHED 22009/zoom
tcp       32      0 kalki-Mi-NoteBook:45952 596.bm-nginx-load:https CLOSE_WAIT  1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:52480 104.26.3.78:https       ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:35066 34.120.72.148:https     ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:48958 151.101.153.253:https   ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:37820 ip33.67-202-110.s:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:49838 a23-57-13-39.depl:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:49740 104.27.118.115:https    ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:48610 72.251.249.14:https     CLOSE_WAIT  1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:36258 a23-9-208-202.dep:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:54604 153.232.73.34.bc.:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:39822 ec2-52-202-62-248:https ESTABLISHED 22009/zoom
tcp        0      0 kalki-Mi-NoteBook:35348 128.199.188.97:https    ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:48908 server-13-227-235:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:51300 bom07s25-in-f14.1:https ESTABLISHED 1877/chrome --type=
tcp        0      0 kalki-Mi-NoteBook:50208 server-13-227-235:https ESTABLISHED 1877/chrome --type=
```

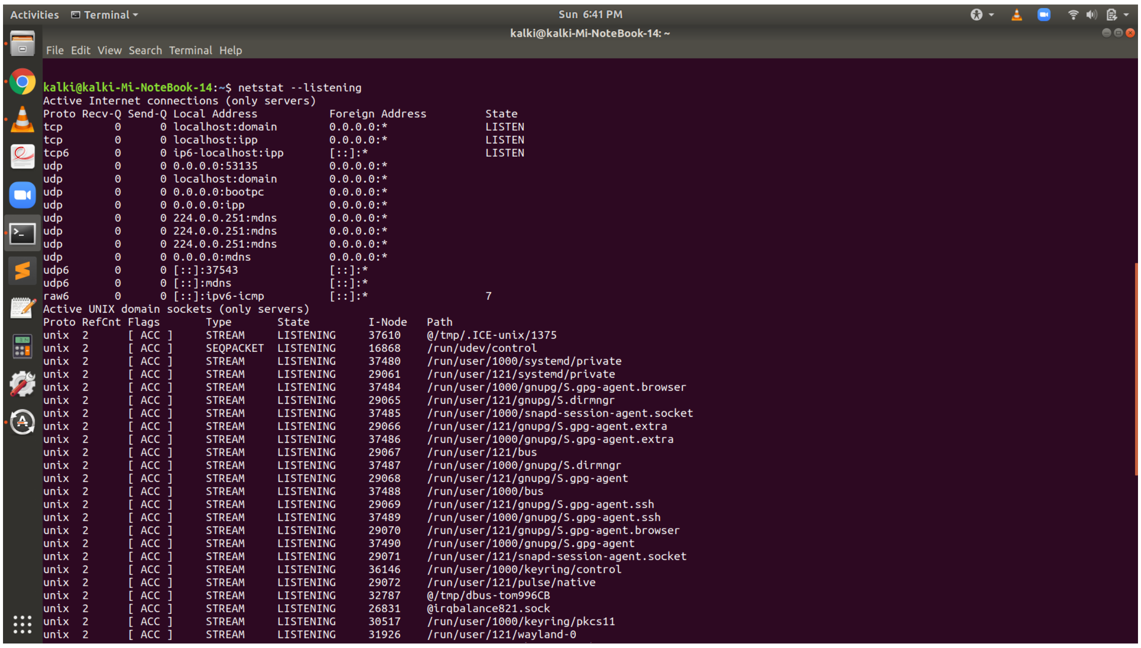
Figure 9: netstat -tcp: To list all tcp ports.



Activities
Terminal
Sun 6:39 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help
Terminal

```
kalki@kalki-Mi-NoteBook-14:~$ netstat -udp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 kalki-Mi-NoteBook:60686 del03s01-in-f2.1e10:443 ESTABLISHED 1877/chrome --type=
udp        0      0 kalki-Mi-NoteBook:38307 bom07s25-in-f14.1e1:443 ESTABLISHED 1877/chrome --type=
udp        0      0 kalki-Mi-NoteBook:38550 bom07s16-in-f2.1e10:443 ESTABLISHED 1877/chrome --type=
udp        0      0 kalki-Mi-NoteBook:55009 bom07s20-in-f6.1e10:443 ESTABLISHED 1877/chrome --type=
udp        0      0 kalki-Mi-NoteBook:35226 del11s05-in-f4.1e10:443 ESTABLISHED 1877/chrome --type=
udp        0      0 kalki-Mi-NoteBook:35474 bom07s16-in-f2.1e10:443 ESTABLISHED 1877/chrome --type=
kalki@kalki-Mi-NoteBook-14:~$ 
```

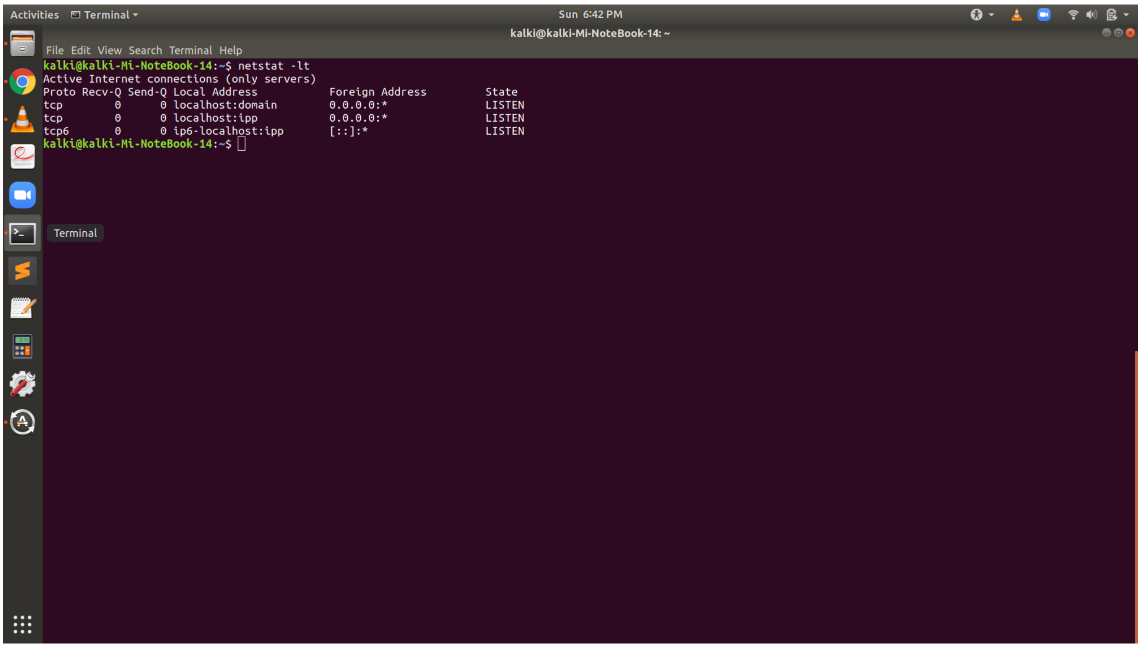
Figure 10: netstat -udp: To list all udp ports.



Activities
Terminal
Sun 6:41 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

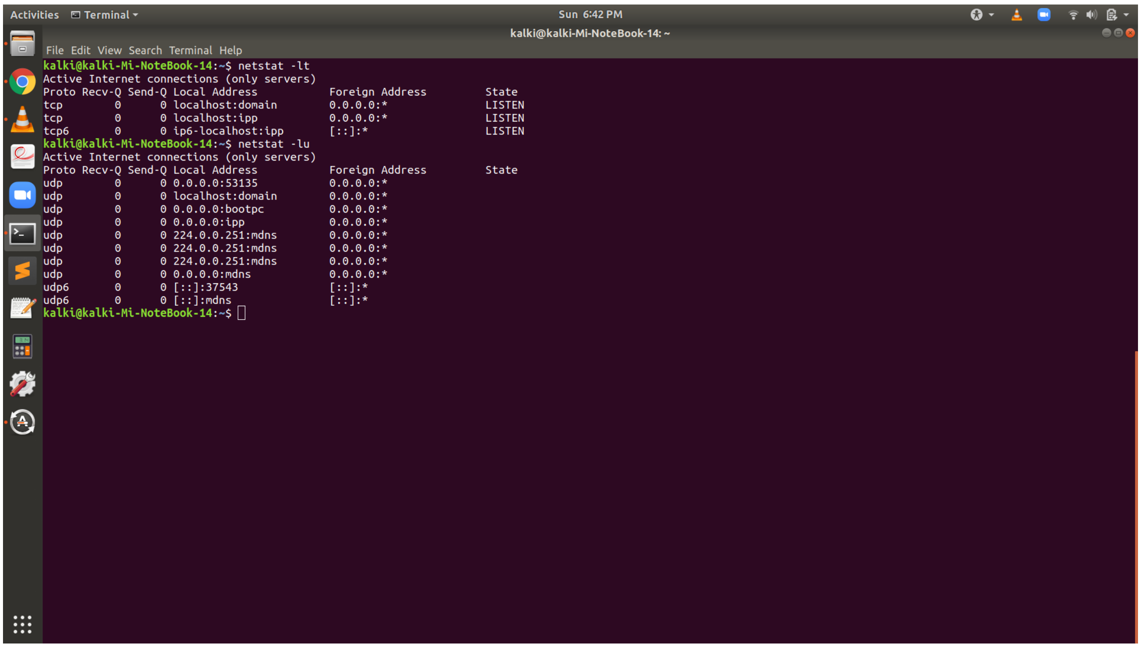
```
kalki@kalki-Mi-NoteBook-14:~$ netstat --listening
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 0.0.0.0:53135           0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp6       0      0 [::]:37543              [::]:*
udp6       0      0 [::]:mdns               [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     37610    @/tmp/.ICE-unix/1375
unix  2      [ ACC ]     SEQPACKET  LISTENING     16868    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     37480    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     29061    /run/user/121/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     37484    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     29065    /run/user/121/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     37485    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     29066    /run/user/121/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     37486    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     29067    /run/user/121/bus
unix  2      [ ACC ]     STREAM     LISTENING     37487    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     29068    /run/user/121/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     37488    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     29069    /run/user/121/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     37489    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     29070    /run/user/121/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     37490    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     29071    /run/user/121/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     36146    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     29072    /run/user/121/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     32787    @/tmp/dbus-tom996CB
unix  2      [ ACC ]     STREAM     LISTENING     26831    @irqbalance821.sock
unix  2      [ ACC ]     STREAM     LISTENING     30517    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     31926    /run/user/121/wayland-0
```

Figure 11: netstat –listening: To list only the listening ports.


Activities
Terminal
Sun 6:42 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help
Terminal

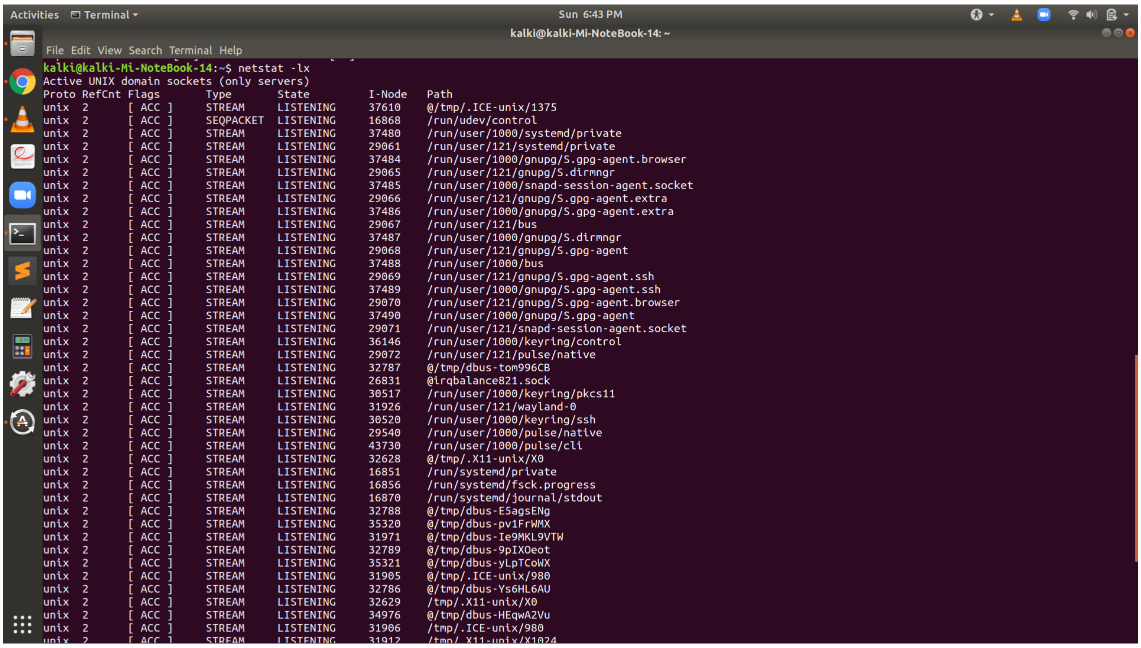
```
kalki@kalki-Mi-NoteBook-14:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
kalki@kalki-Mi-NoteBook-14:~$
```

Figure 12: netstat -lt: To list only the listening tcp ports.


Activities
Terminal
Sun 6:42 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
kalki@kalki-Mi-NoteBook-14:~$ netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:53135           0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp6       0      0 [::]:37543              [::]:*
udp6       0      0 [::]:mdns               [::]:*
kalki@kalki-Mi-NoteBook-14:~$
```

Figure 13: netstat -lu: To list only the listening udp ports.


Activities
Terminal
Sun 6:43 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ netstat -lx
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     37610    @/tmp/.ICE-unix/1375
unix  2      [ ACC ]     SEQPACKET  LISTENING     16868    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     37480    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     29061    /run/user/121/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     37484    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     29065    /run/user/121/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     37485    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     29066    /run/user/121/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     37486    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     29067    /run/user/121/bus
unix  2      [ ACC ]     STREAM     LISTENING     37487    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     29068    /run/user/121/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     37488    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     29069    /run/user/121/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     37489    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     29070    /run/user/121/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     37490    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     29071    /run/user/121/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     36146    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     29072    /run/user/121/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     32787    @/tmp/dbus-tom996CB
unix  2      [ ACC ]     STREAM     LISTENING     26831    @irqbalance821.sock
unix  2      [ ACC ]     STREAM     LISTENING     30517    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     31926    /run/user/121/wayland-0
unix  2      [ ACC ]     STREAM     LISTENING     30520    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     29540    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     43730    /run/user/1000/pulse/cli
unix  2      [ ACC ]     STREAM     LISTENING     32628    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     16851    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     16856    /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     16870    /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM     LISTENING     32788    @/tmp/dbus-E5agsENg
unix  2      [ ACC ]     STREAM     LISTENING     35320    @/tmp/dbus-pv1FrWMX
unix  2      [ ACC ]     STREAM     LISTENING     31971    @/tmp/dbus-Ie9MKL9VTW
unix  2      [ ACC ]     STREAM     LISTENING     32789    @/tmp/dbus-9pIXOeot
unix  2      [ ACC ]     STREAM     LISTENING     35321    @/tmp/dbus-yLpTCoWX
unix  2      [ ACC ]     STREAM     LISTENING     31905    @/tmp/.ICE-unix/980
unix  2      [ ACC ]     STREAM     LISTENING     32786    @/tmp/dbus-Ys6HL6AU
unix  2      [ ACC ]     STREAM     LISTENING     32629    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     34976    @/tmp/dbus-HEqwA2Vu
unix  2      [ ACC ]     STREAM     LISTENING     31906    /tmp/.ICE-unix/980
unix  2      [ ACC ]     STREAM     LISTENING     31912    /tmp/.X11-unix/X1024
```

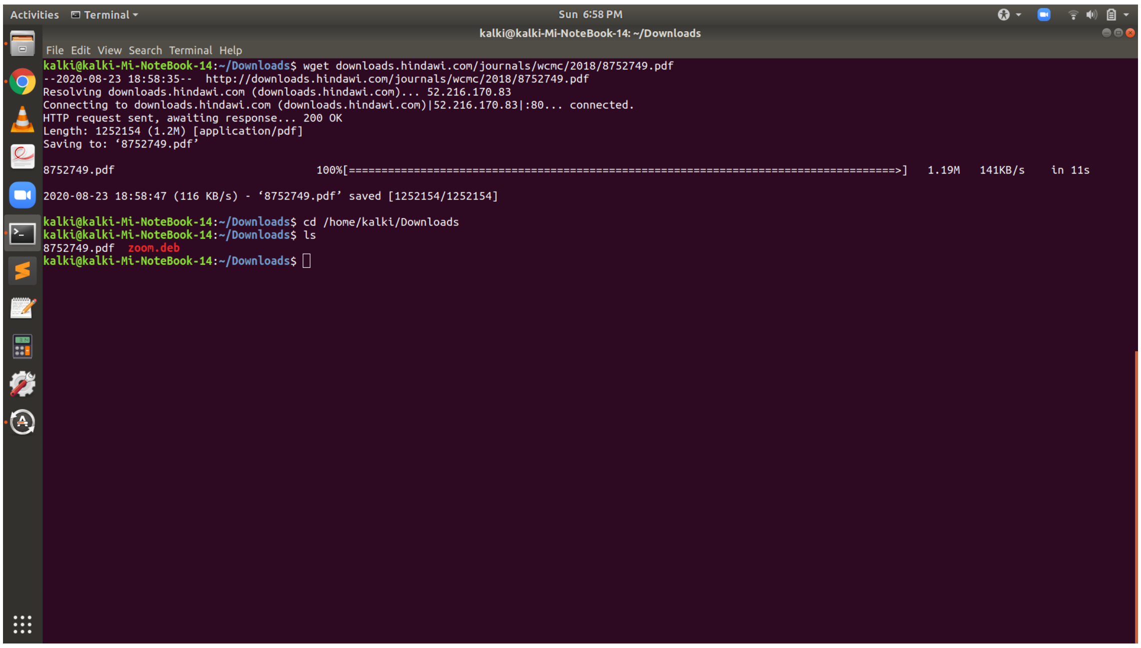
Figure 14: netstat -lx: To list only the listening UNIX ports.

6 wget

- The wget command is a command line utility for downloading files from the Internet. It supports downloading multiple files, downloading in the background, resuming downloads, limiting the bandwidth used for downloads and viewing headers.

- It is also a non-interactive network downloader. It means that it can work in the background, while the user is not logged on. The beauty of this is that most of the browsers require constant user's presence and it may be a hindrance when transferring a lot of data and this is where this command will help to start a retrieval and disconnect from the system letting wget finish the work.

- **Usage:** If a download fails due to network problem, it will keep retrying until the whole file has been retrieved. If the server supports re-getting, it will instruct the server to continue the download from where it left off.



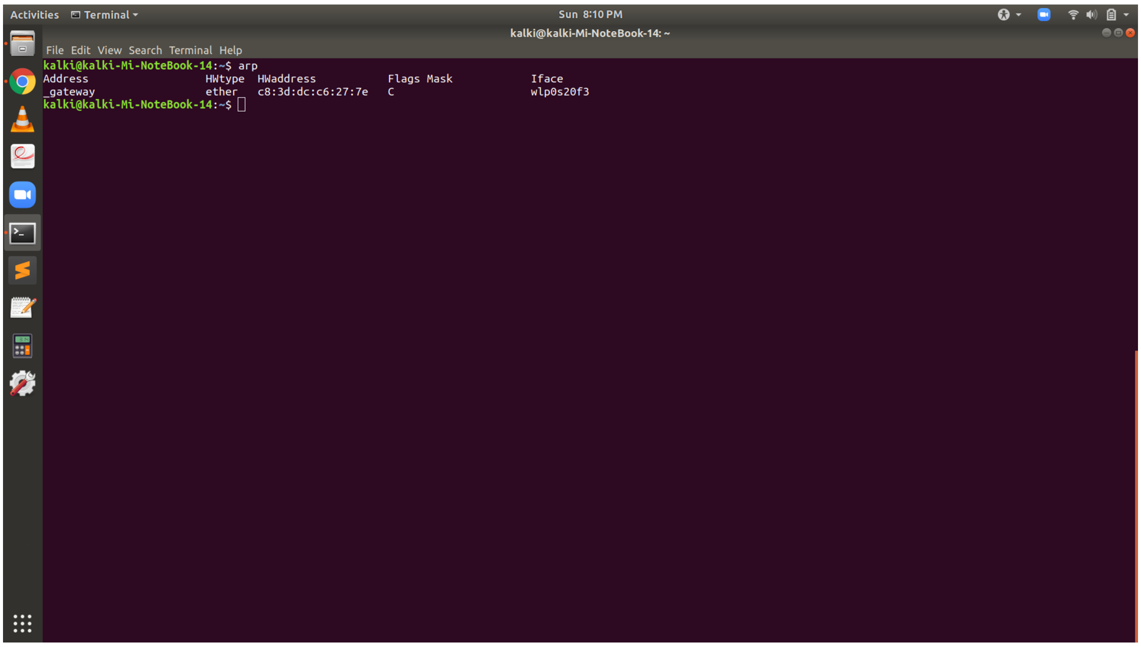
Activities
Terminal
Sun 6:58 PM
kalki@kalki-Mi-NoteBook-14: ~/Downloads
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~/Downloads$ wget downloads.hindawi.com/journals/wcmc/2018/8752749.pdf
--2020-08-23 18:58:35--  http://downloads.hindawi.com/journals/wcmc/2018/8752749.pdf
Resolving downloads.hindawi.com (downloads.hindawi.com)... 52.216.170.83
Connecting to downloads.hindawi.com (downloads.hindawi.com)|52.216.170.83|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1252154 (1.2M) [application/pdf]
Saving to: ‘8752749.pdf’

8752749.pdf                          100%[===================================================================================>]   1.19M   141KB/s    in 11s

2020-08-23 18:58:47 (116 KB/s) - ‘8752749.pdf’ saved [1252154/1252154]

kalki@kalki-Mi-NoteBook-14:~/Downloads$ cd /home/kalki/Downloads
kalki@kalki-Mi-NoteBook-14:~/Downloads$ ls
8752749.pdf  zoom.deb
kalki@kalki-Mi-NoteBook-14:~/Downloads$ 
```

Figure 15: wget url

7 arp

- ARP stands for Address Resolution Protocol.
- It is used to find the media access control address (MAC address) of a network neighbour for a given IPv4 address.
- An ARP cache is a simple mapping of IP addresses to MAC addresses. Each time a computer's TCP/IP stack uses ARP to determine the Media Access Control (MAC) address for an IP address, it records the mapping in the ARP cache so that future ARP lookups go faster.
- arp command is used to manipulate the system ARP cache. More specifically, it manipulates or displays the kernel's IPv4 network neighbour cache and can add entries to the table, delete one, or display the current content.


Activities
Terminal
Sun 8:10 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   c8:3d:dc:c6:27:7e   C                     wlp0s20f3
kalki@kalki-Mi-NoteBook-14:~$ 
```

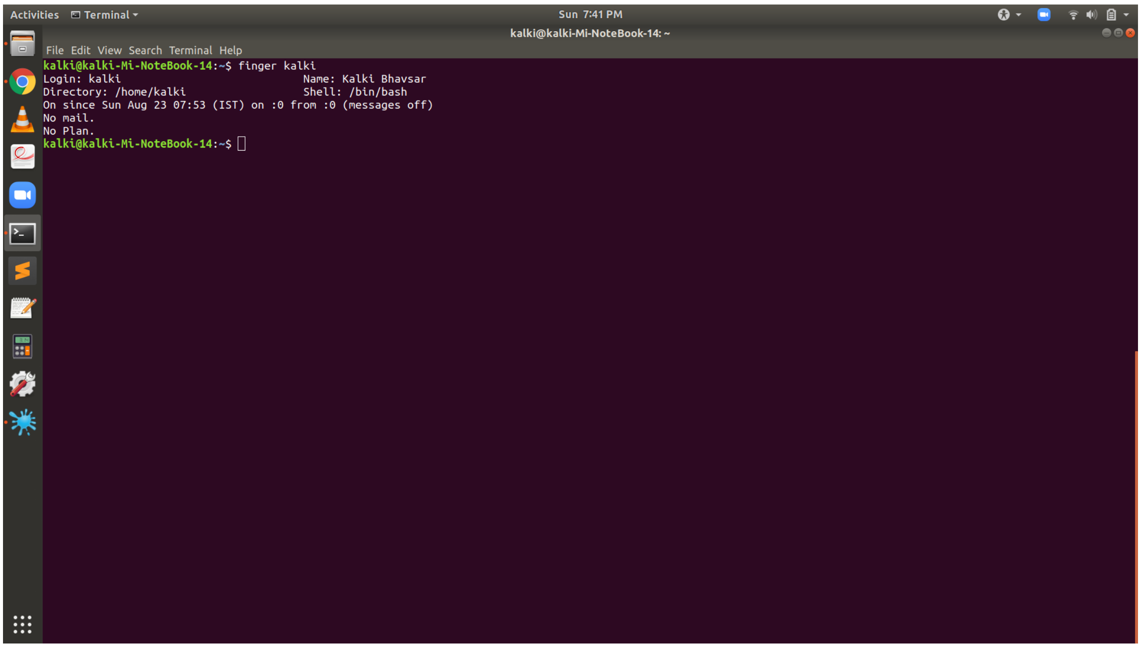
Figure 16: arp

8 ssh

- ssh stands for “Secure Shell”.
- The ssh command provides a secure encrypted connection between two hosts(remote server/system) over an insecure network.
- **Usage:** This connection can also be used for terminal access, file transfers, and for tunneling other applications.

9 finger

- Intallation: $sudo apt-get install finger
- Finger command is a user information lookup command which gives details of all the users logged in. This tool is generally used by system administrators. It provides details like login name, user name, idle time, login time, and in some cases their email address even.
- In short, it displays information about system users.



Activities
Terminal
Sun 7:41 PM
kalki@kalki-Mi-NoteBook-14: ~
File Edit View Search Terminal Help

```
kalki@kalki-Mi-NoteBook-14:~$ finger kalki
Login: kalki                            Name: Kalki Bhavsar
Directory: /home/kalki                  Shell: /bin/bash
On since Sun Aug 23 07:53 (IST) on :0 from :0 (messages off)
No mail.
No Plan.
kalki@kalki-Mi-NoteBook-14:~$
```

Figure 17: finger username

10 telnet

- Telnet is one of the earliest remote login protocols on the Internet. It was initally released in the early days of IP networking in 1969, and was for a long time the default way to access remote networked computers.
- It is a client-server protocol that provides the user a terminal session to the remote host from the telnet client application.
- Since the protocol provides no built-in security measures, it suffers from serious security issues that have limited its usefulness in environments where the network cannot be fully trusted. The use of Telnet over the public Internet should be avoided due to the risk of eavesdropping.
- ssh is a more secure remote login protocol than telnet.