THADOMAL SHAHANI
TSEC
ENGINEERING COLLEGE

Name: Manasi Bhagwat
Roll No: 50
Date: 01/02/2021

# Lab Assignment No:1

**Aim**: To understand basic networking commands.

**Lab Outcome Attained:** To get familiar with the basic network administration commands.

**Theory:**

1. IP config:

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

| Parameters | Description |
|---|---|
| /all | Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections. |
| /displaydns | Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers. |
| /flushdns | Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any |

| | |
|---|---|
| | other entries that have been added dynamically. |
| /showclassid | Displays the DHCP class ID for a specified adapter. |
| /renew | Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the *adapter* parameter is included. |

2. Netstat:

This command displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Netstat is commonly used to display network information of the device.

| | |
|---|---|
| -a | This will display all connection and ports |
| -b | Shows the executable involved in each connection or hearing port |
| -e | This protocol will combine with the -sand display the ethernet statistics |
| -n | This will display the address and the port number in the form of numerical |
| -o | It will display the ID of each connection for the ownership process. |
| -r | It will display the routing table |
| -p | Shows connections for the protocol specified by *Protocol*. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. |

3. NSLookup

It Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The nslookup command-line tool is available only if you have installed the TCP/IP protocol.
The nslookup command displays the name and IP address of the device’s default DNS server.

| Parameter | Description |
|---|---|
| nslookup exit | Exits the nslookup command-line tool. |
| nslookup finger | Connects with the finger server on the current computer. |
| nslookup help | Displays a short summary of subcommands. |
| nslookup ls | Lists information for a DNS domain. |
| nslookup lserver | Changes the default server to the specified DNS domain. |
| nslookup root | Changes the default server to the server for the root of the DNS domain name space. |
| nslookup server | Changes the default server to the specified DNS domain. |

4. Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays, of packets across an Internet Protocol (IP) network. Traceroute proceeds unless all (usually three) sent packets are lost more than twice; then the connection is lost and the route cannot be evaluated.

| Parameter | Description |
|---|---|
| /d | Stops attempts to resolve the IP addresses of intermediate routers to their names. This can speed up the return of results. |
| /h <maximumhops> | Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops. |
| /j <hostlist> | Specifies that echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in <hostlist>. With |

| | |
|---|---|
| | loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the list is 9. The <hostlist> is a series of IP addresses (in dotted decimal notation) separated by spaces. Use this parameter only when tracing IPv4 addresses. |
| /w <timeout> | Specifies the amount of time in milliseconds to wait for the ICMP time Exceeded or echo Reply message corresponding to a given echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds). |
| /4 | Specifies that tracert.exe can use only IPv4 for this trace. |
| /6 | Specifies that tracert.exe can use only IPv6 for this trace. |
| <targetname> | Specifies the destination, identified either by IP address or host name. |
| /? | Displays help at the command prompt. |

5. Route

The route command displays and modifies the entries in the local IP routing table. If used without parameters, route displays help at the command prompt. It displays or modifies the computer's routing table.

| Parameter | Description |
|---|---|
| /f | Clears the routing table of all entries that are not host routes (routes with a netmask of 255.255.255.255), the loopback network route (routes with a destination of 127.0.0.0 and a netmask of 255.0.0.0), or a multicast route (routes with a destination of 224.0.0.0 and a netmask of 240.0.0.0). |
| /p | When used with the add command, the specified route is added to the registry and is used to initialize the IP routing table whenever the TCP/IP protocol is started. By default, added routes are not preserved when the TCP/IP protocol is started. When used with the print command, the list of persistent routes is displayed. This parameter is ignored for all other commands. |
| <command> | Specifies the command you want to run. The valid commands include:<br>• add - Adds a route.<br>• change - Modifies an existing route. |

| | |
|---|---|
| | • delete: - Deletes a route or routes.<br>• print - Prints a route or routes. |
| <destination> | Specifies the network destination of the route. The destination can be an IP network address |

6. SS

The ss command is a tool that is used for displaying network socket related information on a Linux system. The tool displays more detailed information that the netstat command which is used for displaying active socket connections. The ss command can also display even more TCP and state information than most other tools.

| | |
|---|---|
| -a | You can retrieve a list of both listening and non-listening ports. |
| - l | To display listening sockets only. |
| - t | To display all TCP connection. |
| -lt | To have a view of all the listening TCP socket connection. |
| -ua | To view all the UDP socket connections. |
| -lu | To list listening UDP connections. |
| -p | To display the Process IDs related to socket connections. |

## 7. Wget

Wget command is a Linux command line utility that helps us to download the files from the web. We can download the files from web servers using HTTP, HTTPS and FTP protocols. We can use wget in scripts and cronjobs. It supports downloading multiple files , downloading in the background and resuming downloads.

| | |
|---|---|
| <website> | To download the page. |
| -m <website> | To mirror a page |
| -i filename | Read URLs from a local or external file. If - is specified as file, URLs are read from the standard input. |
| -c <website> | Wget can be used to resume an interrupted download file using the -c option |

## 8. Mtr

Mtr which stands for my traceroute is a command line network diagnostic tool that provides the functionality of both the ping and traceroute commands. It is a simple and cross-platform tool that prints information about the entire route that the network packets take, right from the host system to the specified destination system. The mtr command takes an edge over the traceroute command as it also prints the response percentage and the response times for all network hops between the two systems.

| | |
|---|---|
| [domainName/IP] | mtr command displays the hostnames in the traceroute report. |
| -g [domainName/IP] | When you use the g flag with the mtr command, it displays the numeric IP addresses instead of the hostnames in the traceroute report. |
| -b [domainName/IP] | When you use the b flag with the mtr command, it displays both the numeric IP addresses and the hostnames in the traceroute report. |

## 9. Tcpdump

tcpdump is a most powerful and widely used command-line packets sniffer or package-analyzer tool which is used to capture or filter TCP/IP packets that received or transferred over a network on a specific interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. It is available under most of the Linux/Unix based operating systems. tcpdump also gives us a option to save captured packets in a file for future analysis.

| | |
|---|---|
| tcpdump | When you run tcpdump command it will capture all the packets for specified interface |
| -c [n] | Using -c option, you can capture specified number of packets. |
| -D | To list number of available interfaces on the system, run the following command with -D option. |

## 10.Host

host command in Linux system is used for DNS (Domain Name System) lookup operations. In simple words, this command is used to find the IP address of a particular domain name or if you want to find out the domain name of a particular IP address the host command becomes handy. You can also find more specific details of a domain by specifying the corresponding option along with the domain name.

| Parameter | Description |
|---|---|
| -a | The -a (all) option is equivalent to setting the -v option and asking host to make a query of type ANY.. |
| -C | When the -C option is used, host will attempt to display the SOA records for zone name from all the listed authoritative name servers for that zone. The list of name servers is defined by the NS records that are found for the zone. |

| | |
|---|---|
| -d | Verbose output is generated by host when the -d or -v option is used. The two options are equivalent. They have been provided for backwards compatibility. |
| -l | List mode is selected by the -l option. This makes host perform a zone transfer for zone name. Transfer the zone printing out the NS, PTR, and address records (A/AAAA). If combined with -a all records will be printed. |

11.Hostname

The Linux hostname command is used to view or change a system’s domain and hostname. It can also check a computer’s IP address. The hostname is used to distinguish devices within a local network. In addition, computers can be found by others through the hostname, which enables data exchange within a network hostname command in Linux is used to obtain the DNS(Domain Name System) name and set the system’s hostname or NIS(Network Information System) domain name. A hostname is a name which is given to a computer and it attached to the network. Its main purpose is to uniquely identify over a network.

| Parameters | Description |
|---|---|
| -s | Output is computer name |
| -d | Output is domain name of the system |
| -i | IP address for the hostname can also be retrieved |
| hostname | Output is name of the computer and domain name |

12.Ping

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of corresponding echo Reply messages are displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content. You can also use this command to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name isn't, you might have a name resolution problem.

| Parameters | Description |
|---|---|
| target | This is the destination IP address or a hostname user want to ping. |
| -a | This option resolves the hostname of an IP address target. |
| -t | This ping command option will ping the target until you stop it by pressing Ctrl-C. |
| -n count | This option is used to set the number of ICMP Echo Requests to send, from 1 to 4294967295. If -n is not specified, the ping command will return 4 by default. |
| -l size | This option is used to set the size, in bytes, of the echo-request packet from 32 to 65,527. If -l option is not specified, the ping command will send a 32-byte echo request. Option is not specified, the ping command will send a 32-byte echo request. |
| -s count | This option is used to report the time in the Internet Timestamp format, that each echo request is received and an echo reply is sent. The maximum count value is 4, i.e. only the first four hops can be time stamped. |
| -i TTL | This ping command option sets the Time to Live (TTL) value, the maximum value is 255. |

13.<u>ifConfig</u>

ifconfig in short "interface configuration" utility for system/network administration in Unix/Linux operating systems to configure, manage and query network interface parameters via command line interface or in a system configuration scripts. The "ifconfig" command is used for displaying current network configuration information, setting up an ip address, netmask or broadcast address to an network interface, creating an alias for network interface, setting up hardware address and enable or disable network interfaces.

14.<u>Dig</u>

Dig stands for Domain Information Groper is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems. It also perform DNS lookups and displays the answers that are returned from the name server that were queried.

| | |
|---|---|
| -i | use IP6.INT for IPv6 reverse lookups |
| -f filename | Batch mode |
| -b address[#port] | Bind to source address/port |
| -p port | Specify port number |
| -q name | Specify query name |
| -4 | Use IPv4 query transport only |
| -6 | Use IPv6 query transport only |
| -m | Enable memory usage debugging |

15. <u>Whois</u>

whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information.

| | |
|---|---|
| h *HOST* | Connect to WHOIS database host *HOST*. |
| -H | Suppress the display of legal disclaimers. |
| -p *PORT* | When connecting, connect to network port *PORT*. |
| --verbose | Operate verbosely. |
| --help | Display a help message, and exit. |

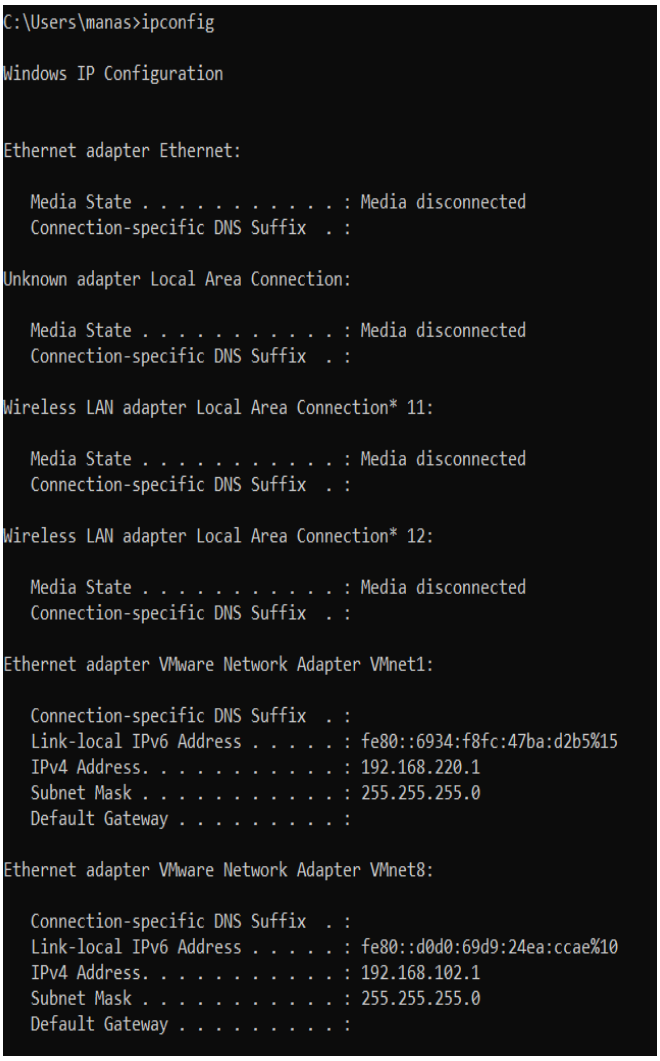
16. <u>ARP</u>

The ARP commands to view, display, or modify the details/information in an ARP table/cache. The ARP cache or table has the dynamic list of IP and MAC addresses of those devices to which your computer has communicated recently in a local network. The purpose of maintaining an ARP table is that when you want to communicate with another device, your device does not need to send the ARP request for the MAC address of that device. The ARP commands also helps to find out the duplicate IP address and invalid entries in an ARP table/cache.

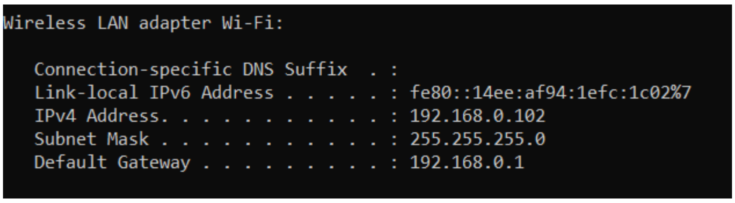
| | |
|---|---|
| -a | This command is used to display the ARP table for a particular IP address. It also shows all the entries of the ARP cache or table. |
| -s | This command is used to add the static entry in the ARP table, which resolves the InetAddr (IP address) to the EtherAddr (physical address). To add a static entry in an ARP table, write arp -s command along with the IP address and MAC address of the device in a command prompt. |
| -g | This command works the same as the arp -a command |
| -d | This command is used when you want to delete an entry from the ARP table for a particular interface. To delete an entry, write arp -d command along with the IP address in a command prompt you want to delete. |

Screenshots:

Ipconfig-

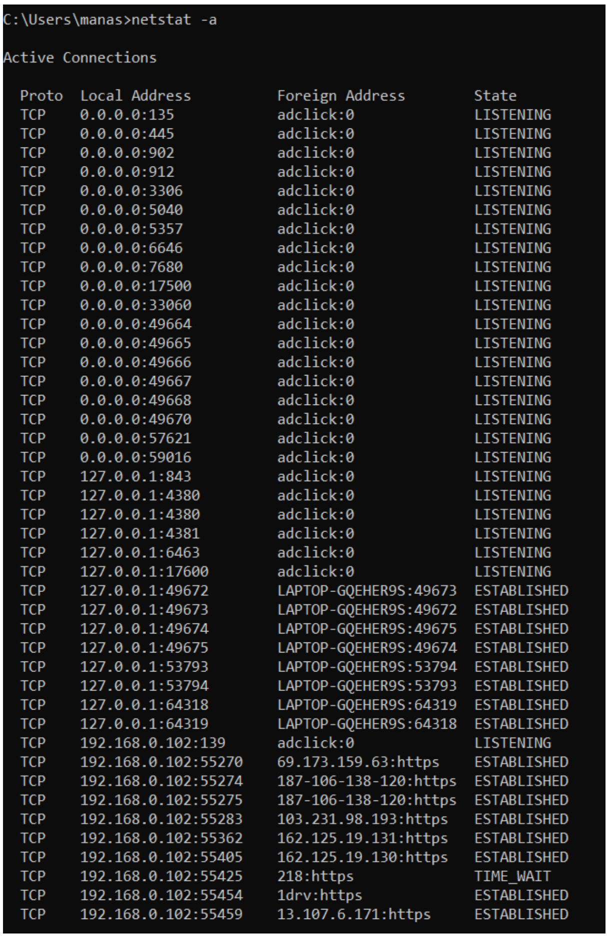


```
C:\Users\manas>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6934:f8fc:47ba:d2b5%15
   IPv4 Address. . . . . . . . . . . : 192.168.220.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d0d0:69d9:24ea:ccae%10
   IPv4 Address. . . . . . . . . . . : 192.168.102.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

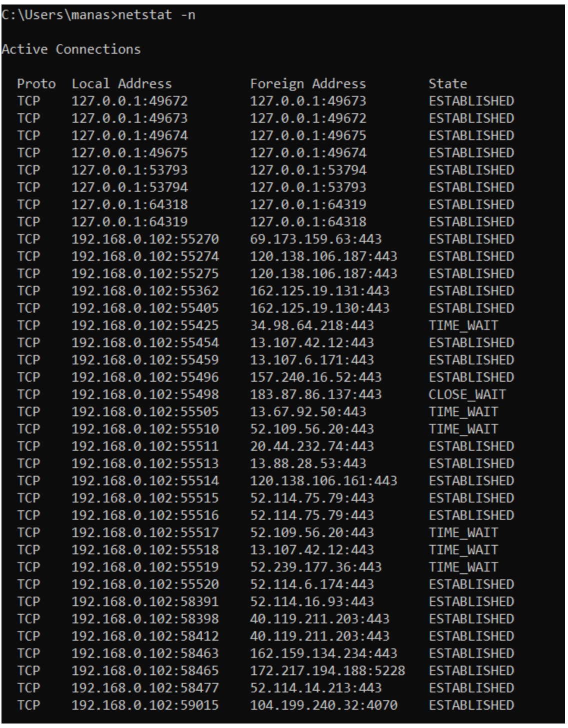


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::14ee:af94:1efc:1c02%7
   IPv4 Address. . . . . . . . . . . : 192.168.0.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

Netstat-

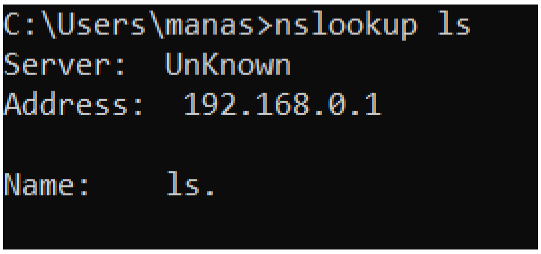


```
C:\Users\manas>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            adclick:0              LISTENING
  TCP    0.0.0.0:445            adclick:0              LISTENING
  TCP    0.0.0.0:902            adclick:0              LISTENING
  TCP    0.0.0.0:912            adclick:0              LISTENING
  TCP    0.0.0.0:3306           adclick:0              LISTENING
  TCP    0.0.0.0:5040           adclick:0              LISTENING
  TCP    0.0.0.0:5357           adclick:0              LISTENING
  TCP    0.0.0.0:6646           adclick:0              LISTENING
  TCP    0.0.0.0:7680           adclick:0              LISTENING
  TCP    0.0.0.0:17500          adclick:0              LISTENING
  TCP    0.0.0.0:33060          adclick:0              LISTENING
  TCP    0.0.0.0:49664          adclick:0              LISTENING
  TCP    0.0.0.0:49665          adclick:0              LISTENING
  TCP    0.0.0.0:49666          adclick:0              LISTENING
  TCP    0.0.0.0:49667          adclick:0              LISTENING
  TCP    0.0.0.0:49668          adclick:0              LISTENING
  TCP    0.0.0.0:49670          adclick:0              LISTENING
  TCP    0.0.0.0:57621          adclick:0              LISTENING
  TCP    0.0.0.0:59016          adclick:0              LISTENING
  TCP    127.0.0.1:843          adclick:0              LISTENING
  TCP    127.0.0.1:4380         adclick:0              LISTENING
  TCP    127.0.0.1:4380         adclick:0              LISTENING
  TCP    127.0.0.1:4381         adclick:0              LISTENING
  TCP    127.0.0.1:6463         adclick:0              LISTENING
  TCP    127.0.0.1:17600        adclick:0              LISTENING
  TCP    127.0.0.1:49672        LAPTOP-GQEHER9S:49673  ESTABLISHED
  TCP    127.0.0.1:49673        LAPTOP-GQEHER9S:49672  ESTABLISHED
  TCP    127.0.0.1:49674        LAPTOP-GQEHER9S:49675  ESTABLISHED
  TCP    127.0.0.1:49675        LAPTOP-GQEHER9S:49674  ESTABLISHED
  TCP    127.0.0.1:53793        LAPTOP-GQEHER9S:53794  ESTABLISHED
  TCP    127.0.0.1:53794        LAPTOP-GQEHER9S:53793  ESTABLISHED
  TCP    127.0.0.1:64318        LAPTOP-GQEHER9S:64319  ESTABLISHED
  TCP    127.0.0.1:64319        LAPTOP-GQEHER9S:64318  ESTABLISHED
  TCP    192.168.0.102:139      adclick:0              LISTENING
  TCP    192.168.0.102:55270    69.173.159.63:https    ESTABLISHED
  TCP    192.168.0.102:55274    187-106-138-120:https  ESTABLISHED
  TCP    192.168.0.102:55275    187-106-138-120:https  ESTABLISHED
  TCP    192.168.0.102:55283    103.231.98.193:https   ESTABLISHED
  TCP    192.168.0.102:55362    162.125.19.131:https   ESTABLISHED
  TCP    192.168.0.102:55405    162.125.19.130:https   ESTABLISHED
  TCP    192.168.0.102:55425    218:https              TIME_WAIT
  TCP    192.168.0.102:55454    1drv:https             ESTABLISHED
  TCP    192.168.0.102:55459    13.107.6.171:https     ESTABLISHED
```



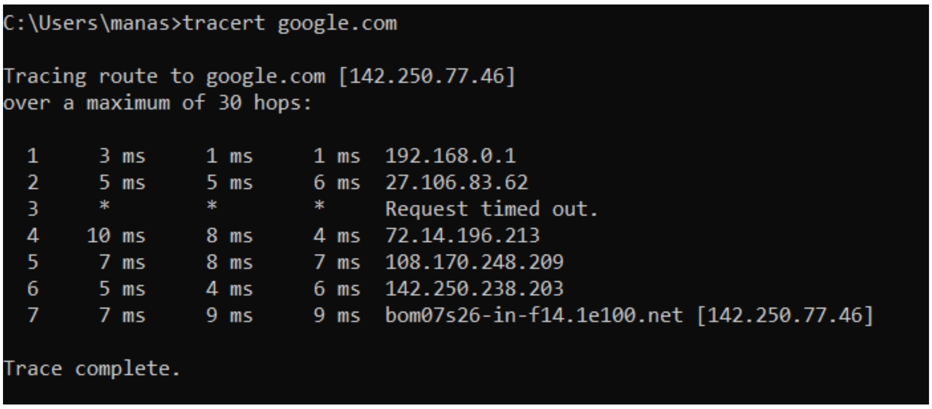
```
C:\Users\manas>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49672        127.0.0.1:49673        ESTABLISHED
  TCP    127.0.0.1:49673        127.0.0.1:49672        ESTABLISHED
  TCP    127.0.0.1:49674        127.0.0.1:49675        ESTABLISHED
  TCP    127.0.0.1:49675        127.0.0.1:49674        ESTABLISHED
  TCP    127.0.0.1:53793        127.0.0.1:53794        ESTABLISHED
  TCP    127.0.0.1:53794        127.0.0.1:53793        ESTABLISHED
  TCP    127.0.0.1:64318        127.0.0.1:64319        ESTABLISHED
  TCP    127.0.0.1:64319        127.0.0.1:64318        ESTABLISHED
  TCP    192.168.0.102:55270    69.173.159.63:443      ESTABLISHED
  TCP    192.168.0.102:55274    120.138.106.187:443    ESTABLISHED
  TCP    192.168.0.102:55275    120.138.106.187:443    ESTABLISHED
  TCP    192.168.0.102:55362    162.125.19.131:443     ESTABLISHED
  TCP    192.168.0.102:55405    162.125.19.130:443     ESTABLISHED
  TCP    192.168.0.102:55425    34.98.64.218:443       TIME_WAIT
  TCP    192.168.0.102:55454    13.107.42.12:443       ESTABLISHED
  TCP    192.168.0.102:55459    13.107.6.171:443       ESTABLISHED
  TCP    192.168.0.102:55496    157.240.16.52:443      ESTABLISHED
  TCP    192.168.0.102:55498    183.87.86.137:443      CLOSE_WAIT
  TCP    192.168.0.102:55505    13.67.92.50:443        TIME_WAIT
  TCP    192.168.0.102:55510    52.109.56.20:443       TIME_WAIT
  TCP    192.168.0.102:55511    20.44.232.74:443       ESTABLISHED
  TCP    192.168.0.102:55513    13.88.28.53:443        ESTABLISHED
  TCP    192.168.0.102:55514    120.138.106.161:443    ESTABLISHED
  TCP    192.168.0.102:55515    52.114.75.79:443       ESTABLISHED
  TCP    192.168.0.102:55516    52.114.75.79:443       ESTABLISHED
  TCP    192.168.0.102:55517    52.109.56.20:443       TIME_WAIT
  TCP    192.168.0.102:55518    13.107.42.12:443       TIME_WAIT
  TCP    192.168.0.102:55519    52.239.177.36:443      TIME_WAIT
  TCP    192.168.0.102:55520    52.114.6.174:443       ESTABLISHED
  TCP    192.168.0.102:58391    52.114.16.93:443       ESTABLISHED
  TCP    192.168.0.102:58398    40.119.211.203:443     ESTABLISHED
  TCP    192.168.0.102:58412    40.119.211.203:443     ESTABLISHED
  TCP    192.168.0.102:58463    162.159.134.234:443    ESTABLISHED
  TCP    192.168.0.102:58465    172.217.194.188:5228   ESTABLISHED
  TCP    192.168.0.102:58477    52.114.14.213:443      ESTABLISHED
  TCP    192.168.0.102:59015    104.199.240.32:4070    ESTABLISHED
```

Nslookup-



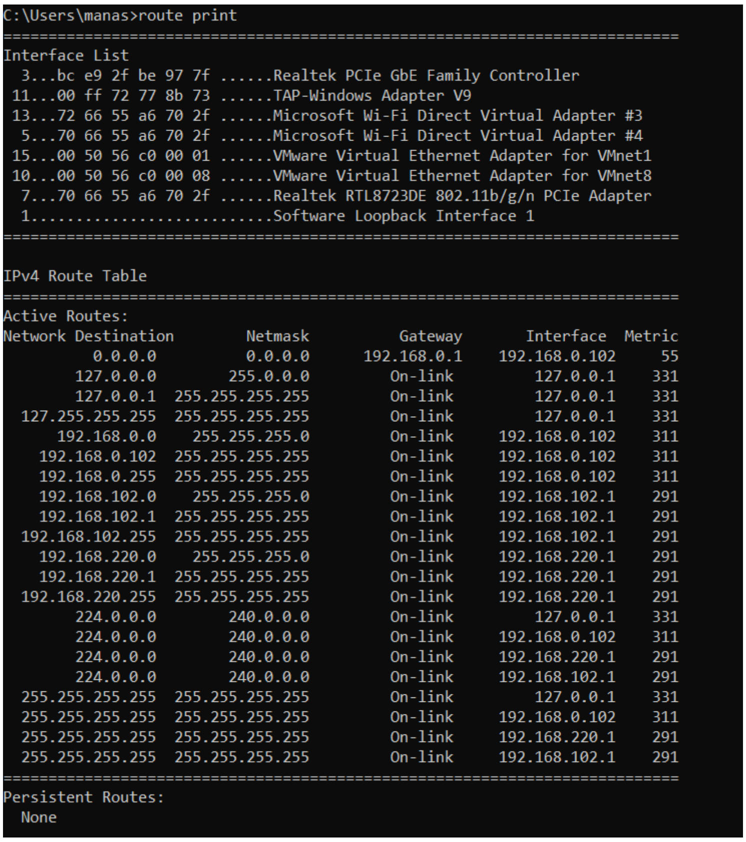
```
C:\Users\manas>nslookup ls
Server:  UnKnown
Address:  192.168.0.1

Name:    ls.
```

Traceroute-

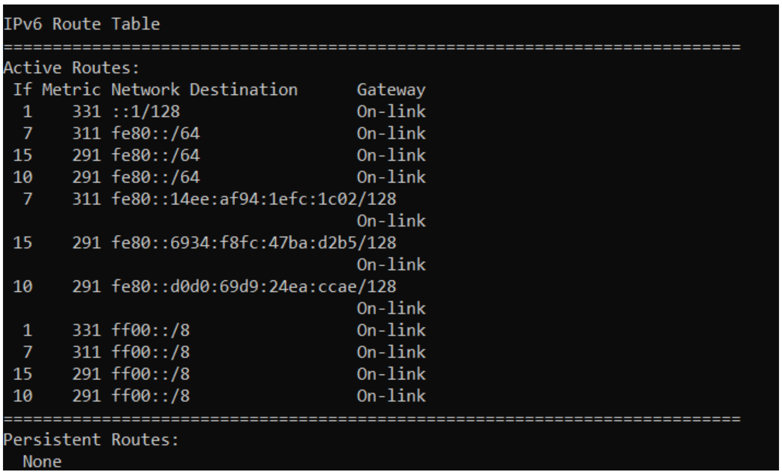


```
C:\Users\manas>tracert google.com

Tracing route to google.com [142.250.77.46]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  192.168.0.1
  2     5 ms     5 ms     6 ms  27.106.83.62
  3     *        *        *     Request timed out.
  4    10 ms     8 ms     4 ms  72.14.196.213
  5     7 ms     8 ms     7 ms  108.170.248.209
  6     5 ms     4 ms     6 ms  142.250.238.203
  7     7 ms     9 ms     9 ms  bom07s26-in-f14.1e100.net [142.250.77.46]

Trace complete.
```

Route-

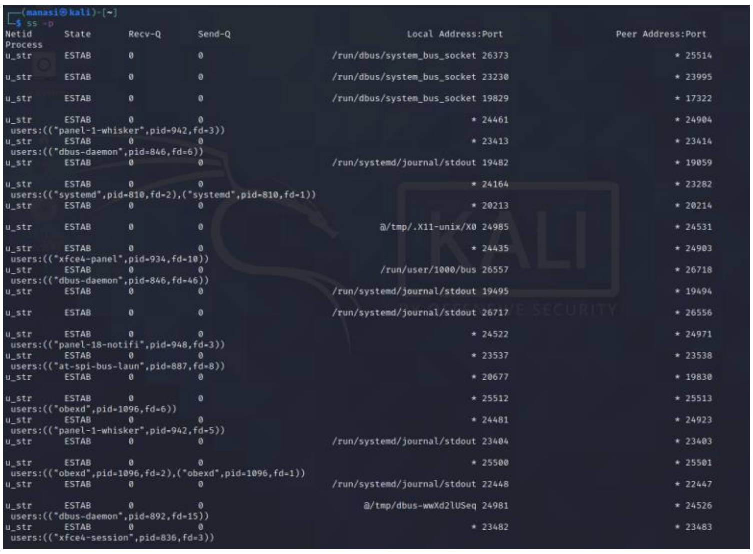


```
C:\Users\manas>route print
===========================================================================
Interface List
  3...bc e9 2f be 97 7f ......Realtek PCIe GbE Family Controller
 11...00 ff 72 77 8b 73 ......TAP-Windows Adapter V9
 13...72 66 55 a6 70 2f ......Microsoft Wi-Fi Direct Virtual Adapter #3
  5...70 66 55 a6 70 2f ......Microsoft Wi-Fi Direct Virtual Adapter #4
 15...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 10...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  7...70 66 55 a6 70 2f ......Realtek RTL8723DE 802.11b/g/n PCIe Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.102     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link     192.168.0.102    311
    192.168.0.102  255.255.255.255         On-link     192.168.0.102    311
    192.168.0.255  255.255.255.255         On-link     192.168.0.102    311
    192.168.102.0    255.255.255.0         On-link     192.168.102.1    291
    192.168.102.1  255.255.255.255         On-link     192.168.102.1    291
  192.168.102.255  255.255.255.255         On-link     192.168.102.1    291
    192.168.220.0    255.255.255.0         On-link     192.168.220.1    291
    192.168.220.1  255.255.255.255         On-link     192.168.220.1    291
  192.168.220.255  255.255.255.255         On-link     192.168.220.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.0.102    311
        224.0.0.0        240.0.0.0         On-link     192.168.220.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.102.1    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.0.102    311
  255.255.255.255  255.255.255.255         On-link     192.168.220.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.102.1    291
===========================================================================
Persistent Routes:
  None
```

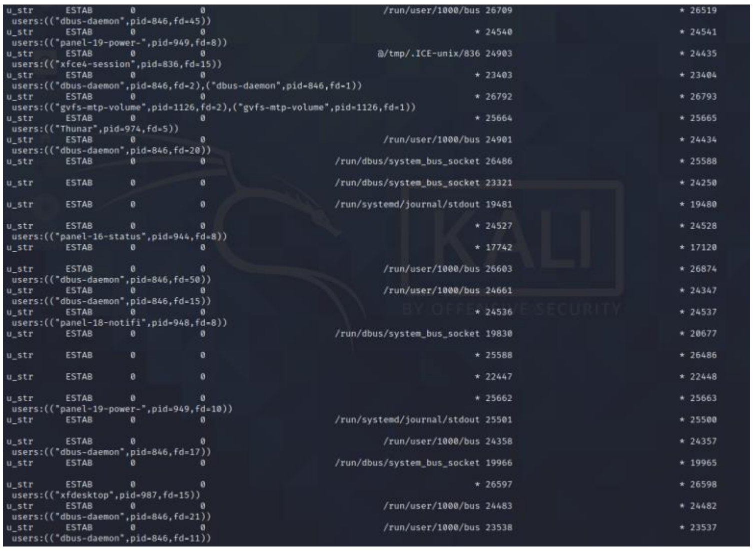


```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  7    311 fe80::/64                On-link
 15    291 fe80::/64                On-link
 10    291 fe80::/64                On-link
  7    311 fe80::14ee:af94:1efc:1c02/128
                                    On-link
 15    291 fe80::6934:f8fc:47ba:d2b5/128
                                    On-link
 10    291 fe80::d0d0:69d9:24ea:ccae/128
                                    On-link
  1    331 ff00::/8                 On-link
  7    311 ff00::/8                 On-link
 15    291 ff00::/8                 On-link
 10    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

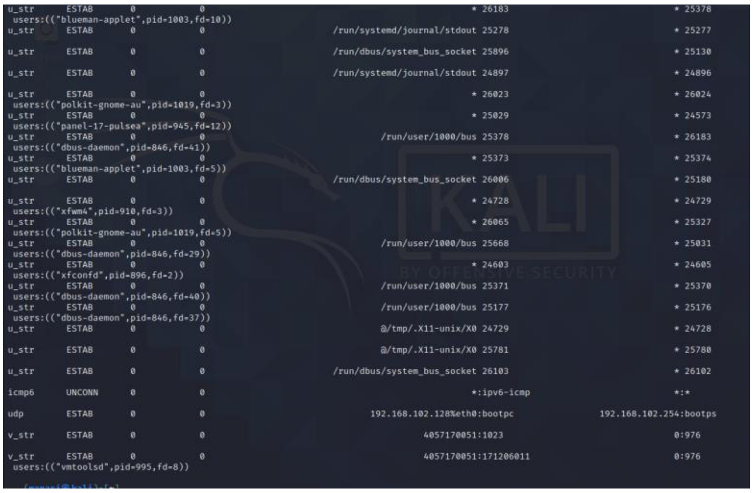
Ss-



```
┌──(manasi㉿kali)-[~]
└─$ ss -p
Netid     State      Recv-Q      Send-Q                     Local Address:Port                     Peer Address:Port
Process
u_str     ESTAB      0           0            /run/dbus/system_bus_socket 26373                              * 25514

u_str     ESTAB      0           0            /run/dbus/system_bus_socket 23230                              * 23995

u_str     ESTAB      0           0            /run/dbus/system_bus_socket 19829                              * 17322

u_str     ESTAB      0           0                                      * 24461                              * 24904
 users:(("panel-1-whisker",pid=942,fd=3))
u_str     ESTAB      0           0                                      * 23413                              * 23414
 users:(("dbus-daemon",pid=846,fd=6))
u_str     ESTAB      0           0            /run/systemd/journal/stdout 19482                              * 19059

u_str     ESTAB      0           0                                      * 24164                              * 23282
 users:(("systemd",pid=810,fd=2),("systemd",pid=810,fd=1))
u_str     ESTAB      0           0                                      * 20213                              * 20214

u_str     ESTAB      0           0                   @/tmp/.X11-unix/X0 24985                              * 24531

u_str     ESTAB      0           0                                      * 24435                              * 24903
 users:(("xfce4-panel",pid=934,fd=10))
u_str     ESTAB      0           0                     /run/user/1000/bus 26557                              * 26718
 users:(("dbus-daemon",pid=846,fd=46))
u_str     ESTAB      0           0            /run/systemd/journal/stdout 19495                              * 19494

u_str     ESTAB      0           0            /run/systemd/journal/stdout 26717                              * 26556

u_str     ESTAB      0           0                                      * 24522                              * 24971
 users:(("panel-18-notifi",pid=948,fd=3))
u_str     ESTAB      0           0                                      * 23537                              * 23538
 users:(("at-spi-bus-laun",pid=887,fd=8))
u_str     ESTAB      0           0                                      * 20677                              * 19830

u_str     ESTAB      0           0                                      * 25512                              * 25513
 users:(("obexd",pid=1096,fd=6))
u_str     ESTAB      0           0                                      * 24481                              * 24923
 users:(("panel-1-whisker",pid=942,fd=5))
u_str     ESTAB      0           0            /run/systemd/journal/stdout 23404                              * 23403

u_str     ESTAB      0           0                                      * 25500                              * 25501
 users:(("obexd",pid=1096,fd=2),("obexd",pid=1096,fd=1))
u_str     ESTAB      0           0            /run/systemd/journal/stdout 22448                              * 22447

u_str     ESTAB      0           0                @/tmp/dbus-wwXd2lUSeq 24981                              * 24526
 users:(("dbus-daemon",pid=892,fd=15))
u_str     ESTAB      0           0                                      * 23482                              * 23483
 users:(("xfce4-session",pid=836,fd=3))
```

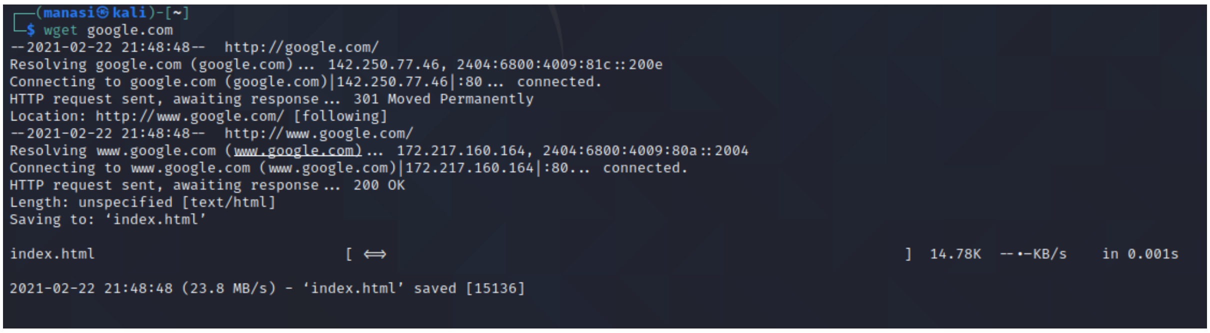


```
u_str     ESTAB      0           0                     /run/user/1000/bus 26709                              * 26519
 users:(("dbus-daemon",pid=846,fd=45))
u_str     ESTAB      0           0                                      * 24540                              * 24541
 users:(("panel-19-power-",pid=949,fd=8))
u_str     ESTAB      0           0                 @/tmp/.ICE-unix/836 24903                              * 24435
 users:(("xfce4-session",pid=836,fd=15))
u_str     ESTAB      0           0                                      * 23403                              * 23404
 users:(("dbus-daemon",pid=846,fd=2),("dbus-daemon",pid=846,fd=1))
u_str     ESTAB      0           0                                      * 26792                              * 26793
 users:(("gvfs-mtp-volume",pid=1126,fd=2),("gvfs-mtp-volume",pid=1126,fd=1))
u_str     ESTAB      0           0                                      * 25664                              * 25665
 users:(("Thunar",pid=974,fd=5))
u_str     ESTAB      0           0                     /run/user/1000/bus 24901                              * 24434
 users:(("dbus-daemon",pid=846,fd=20))
u_str     ESTAB      0           0            /run/dbus/system_bus_socket 26486                              * 25588

u_str     ESTAB      0           0            /run/dbus/system_bus_socket 23321                              * 24250

u_str     ESTAB      0           0            /run/systemd/journal/stdout 19481                              * 19480

u_str     ESTAB      0           0                                      * 24527                              * 24528
 users:(("panel-16-status",pid=944,fd=8))
u_str     ESTAB      0           0                                      * 17742                              * 17120

u_str     ESTAB      0           0                     /run/user/1000/bus 26603                              * 26874
 users:(("dbus-daemon",pid=846,fd=50))
u_str     ESTAB      0           0                     /run/user/1000/bus 24661                              * 24347
 users:(("dbus-daemon",pid=846,fd=15))
u_str     ESTAB      0           0                                      * 24536                              * 24537
 users:(("panel-18-notifi",pid=948,fd=8))
u_str     ESTAB      0           0            /run/dbus/system_bus_socket 19830                              * 20677

u_str     ESTAB      0           0                                      * 25588                              * 26486

u_str     ESTAB      0           0                                      * 22447                              * 22448

u_str     ESTAB      0           0                                      * 25662                              * 25663
 users:(("panel-19-power-",pid=949,fd=10))
u_str     ESTAB      0           0            /run/systemd/journal/stdout 25501                              * 25500

u_str     ESTAB      0           0                     /run/user/1000/bus 24358                              * 24357
 users:(("dbus-daemon",pid=846,fd=17))
u_str     ESTAB      0           0            /run/dbus/system_bus_socket 19966                              * 19965

u_str     ESTAB      0           0                                      * 26597                              * 26598
 users:(("xfdesktop",pid=987,fd=15))
u_str     ESTAB      0           0                     /run/user/1000/bus 24483                              * 24482
 users:(("dbus-daemon",pid=846,fd=21))
u_str     ESTAB      0           0                     /run/user/1000/bus 23538                              * 23537
 users:(("dbus-daemon",pid=846,fd=11))
```



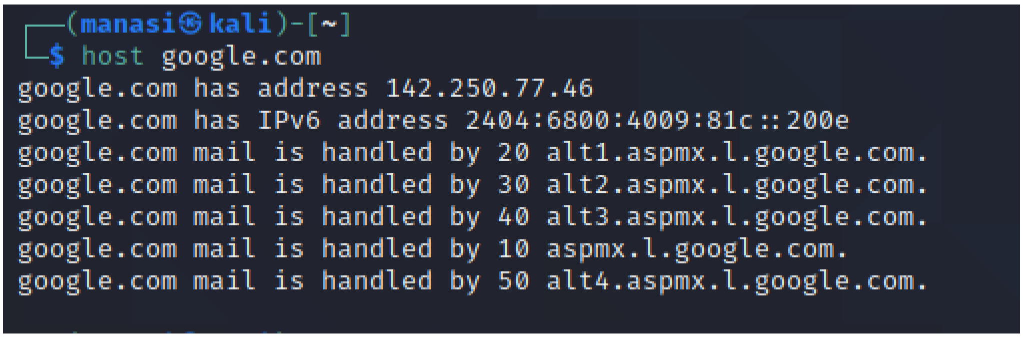
```
u_str     ESTAB      0           0                                      * 26183                              * 25378
 users:(("blueman-applet",pid=1003,fd=10))
u_str     ESTAB      0           0            /run/systemd/journal/stdout 25278                              * 25277

u_str     ESTAB      0           0            /run/dbus/system_bus_socket 25896                              * 25130

u_str     ESTAB      0           0            /run/systemd/journal/stdout 24897                              * 24896

u_str     ESTAB      0           0                                      * 26023                              * 26024
 users:(("polkit-gnome-au",pid=1019,fd=3))
u_str     ESTAB      0           0                                      * 25029                              * 24573
 users:(("panel-17-pulsea",pid=945,fd=12))
u_str     ESTAB      0           0                     /run/user/1000/bus 25378                              * 26183
 users:(("dbus-daemon",pid=846,fd=41))
u_str     ESTAB      0           0                                      * 25373                              * 25374
 users:(("blueman-applet",pid=1003,fd=5))
u_str     ESTAB      0           0            /run/dbus/system_bus_socket 26006                              * 25180

u_str     ESTAB      0           0                                      * 24728                              * 24729
 users:(("xfwm4",pid=910,fd=3))
u_str     ESTAB      0           0                                      * 26065                              * 25327
 users:(("polkit-gnome-au",pid=1019,fd=5))
u_str     ESTAB      0           0                     /run/user/1000/bus 25668                              * 25031
 users:(("dbus-daemon",pid=846,fd=29))
u_str     ESTAB      0           0                                      * 24603                              * 24605
 users:(("xfconfd",pid=896,fd=2))
u_str     ESTAB      0           0                     /run/user/1000/bus 25371                              * 25370
 users:(("dbus-daemon",pid=846,fd=40))
u_str     ESTAB      0           0                     /run/user/1000/bus 25177                              * 25176
 users:(("dbus-daemon",pid=846,fd=37))
u_str     ESTAB      0           0                   @/tmp/.X11-unix/X0 24729                              * 24728

u_str     ESTAB      0           0                   @/tmp/.X11-unix/X0 25781                              * 25780

u_str     ESTAB      0           0            /run/dbus/system_bus_socket 26103                              * 26102

icmp6     UNCONN     0           0                                  *:ipv6-icmp                            *:*

udp       ESTAB      0           0              192.168.102.128%eth0:bootpc             192.168.102.254:bootps

v_str     ESTAB      0           0                          4057170051:1023                            0:976

v_str     ESTAB      0           0                     4057170051:171206011                            0:976
 users:(("vmtoolsd",pid=995,fd=8))

┌──(manasi㉿kali)-[~]
```

## Wget-



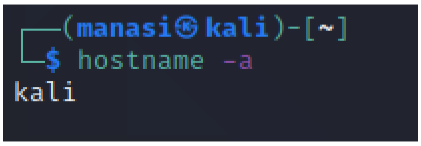
```
┌──(manasi㉿kali)-[~]
└─$ wget google.com
--2021-02-22 21:48:48--  http://google.com/
Resolving google.com (google.com)... 142.250.77.46, 2404:6800:4009:81c::200e
Connecting to google.com (google.com)|142.250.77.46|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2021-02-22 21:48:48--  http://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.160.164, 2404:6800:4009:80a::2004
Connecting to www.google.com (www.google.com)|172.217.160.164|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html’

index.html                      [ <=>                                                  ]  14.78K  --.-KB/s    in 0.001s

2021-02-22 21:48:48 (23.8 MB/s) - ‘index.html’ saved [15136]
```

## Host-



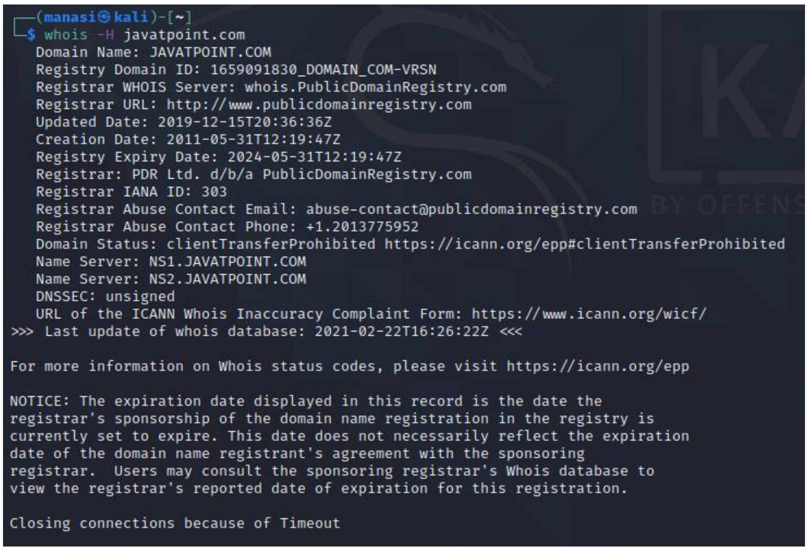
```
┌──(manasi㉿kali)-[~]
└─$ host google.com
google.com has address 142.250.77.46
google.com has IPv6 address 2404:6800:4009:81c::200e
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
```

## Hostname-



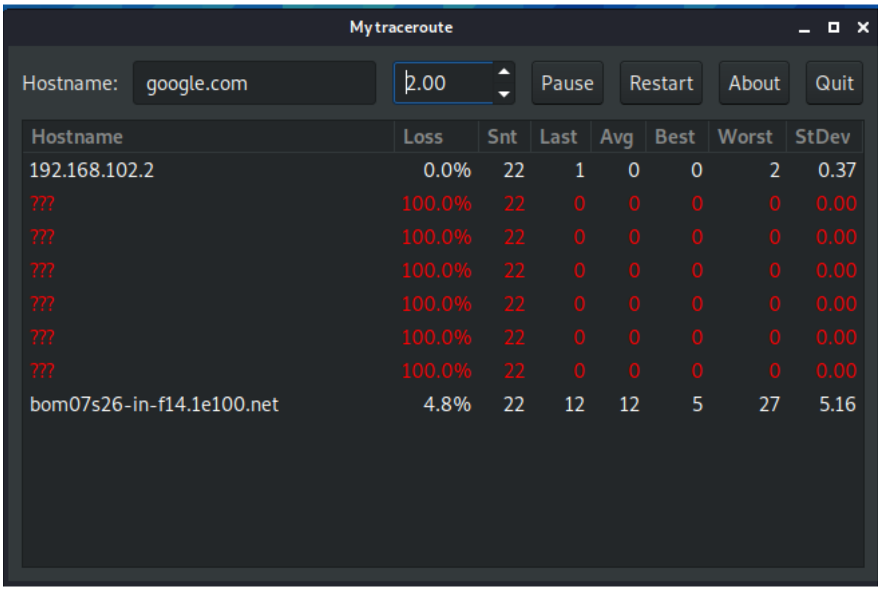
```
┌──(manasi㉿kali)-[~]
└─$ hostname -a
kali
```

## Whois-



```
┌──(manasi㉿kali)-[~]
└─$ whois -H javatpoint.com
   Domain Name: JAVATPOINT.COM
   Registry Domain ID: 1659091830_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.PublicDomainRegistry.com
   Registrar URL: http://www.publicdomainregistry.com
   Updated Date: 2019-12-15T20:36:36Z
   Creation Date: 2011-05-31T12:19:47Z
   Registry Expiry Date: 2024-05-31T12:19:47Z
   Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
   Registrar IANA ID: 303
   Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
   Registrar Abuse Contact Phone: +1.2013775952
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.JAVATPOINT.COM
   Name Server: NS2.JAVATPOINT.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-02-22T16:26:22Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

Closing connections because of Timeout
```

Mtr-

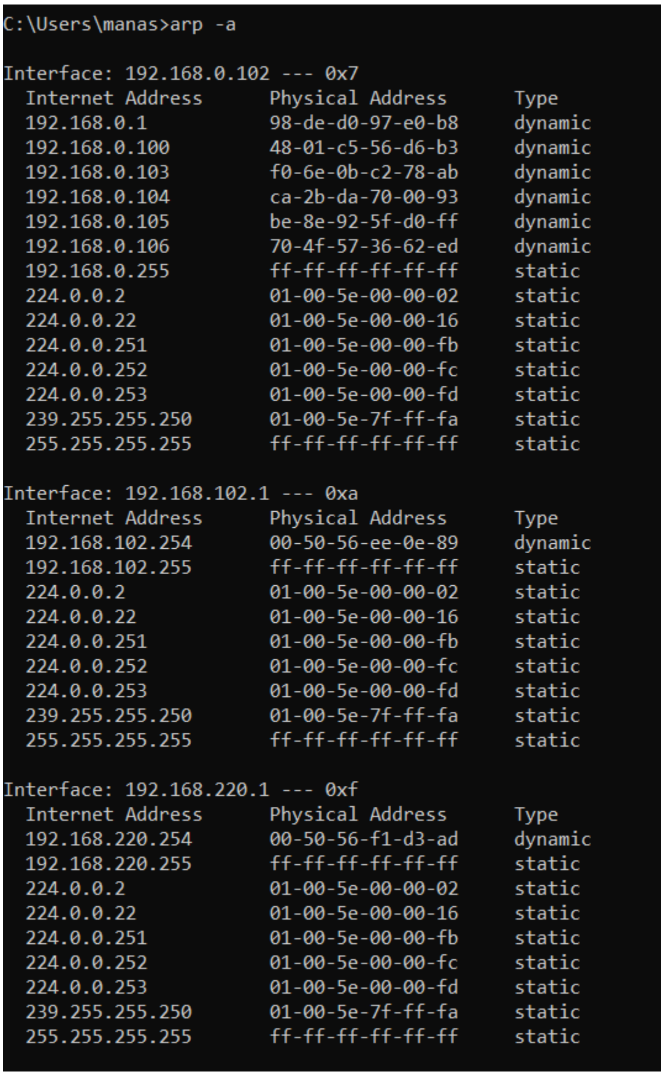


Hostname: google.com

2.00

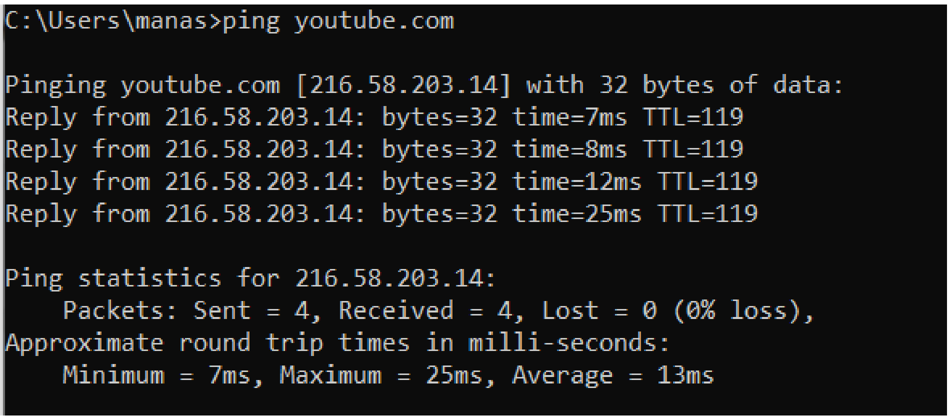
| Hostname | Loss | Snt | Last | Avg | Best | Worst | StDev |
|---|---|---|---|---|---|---|---|
| 192.168.102.2 | 0.0% | 22 | 1 | 0 | 0 | 2 | 0.37 |
| ??? | 100.0% | 22 | 0 | 0 | 0 | 0 | 0.00 |
| ??? | 100.0% | 22 | 0 | 0 | 0 | 0 | 0.00 |
| ??? | 100.0% | 22 | 0 | 0 | 0 | 0 | 0.00 |
| ??? | 100.0% | 22 | 0 | 0 | 0 | 0 | 0.00 |
| ??? | 100.0% | 22 | 0 | 0 | 0 | 0 | 0.00 |
| ??? | 100.0% | 22 | 0 | 0 | 0 | 0 | 0.00 |
| bom07s26-in-f14.1e100.net | 4.8% | 22 | 12 | 12 | 5 | 27 | 5.16 |

Arp-



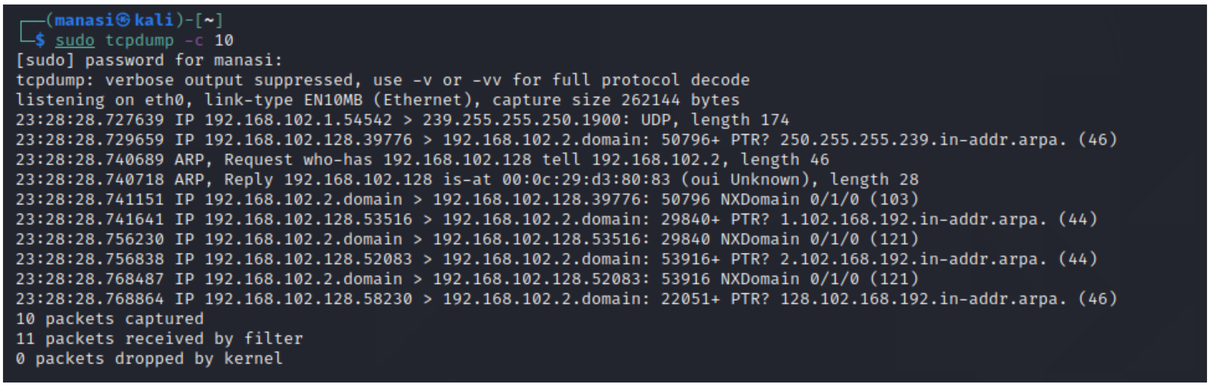
```
C:\Users\manas>arp -a

Interface: 192.168.0.102 --- 0x7
  Internet Address      Physical Address      Type
  192.168.0.1           98-de-d0-97-e0-b8     dynamic
  192.168.0.100         48-01-c5-56-d6-b3     dynamic
  192.168.0.103         f0-6e-0b-c2-78-ab     dynamic
  192.168.0.104         ca-2b-da-70-00-93     dynamic
  192.168.0.105         be-8e-92-5f-d0-ff     dynamic
  192.168.0.106         70-4f-57-36-62-ed     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.102.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.102.254       00-50-56-ee-0e-89     dynamic
  192.168.102.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.220.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.220.254       00-50-56-f1-d3-ad     dynamic
  192.168.220.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Ping-



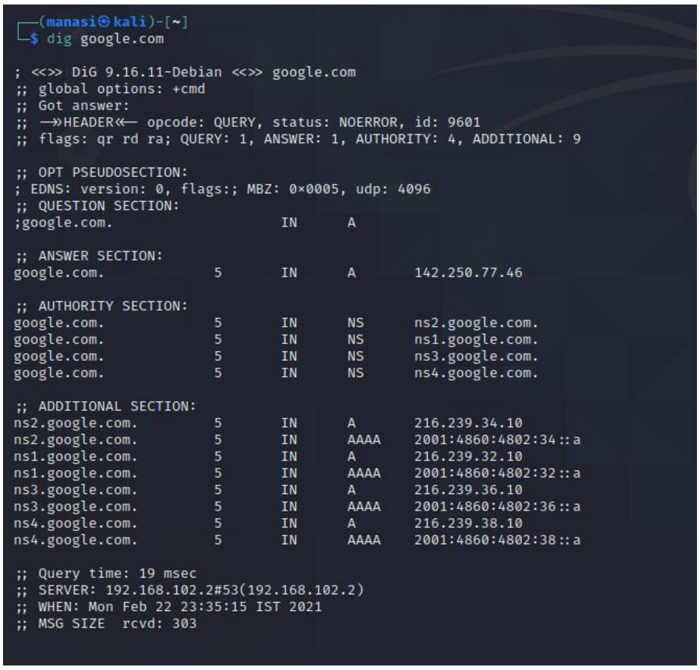
```
C:\Users\manas>ping youtube.com

Pinging youtube.com [216.58.203.14] with 32 bytes of data:
Reply from 216.58.203.14: bytes=32 time=7ms TTL=119
Reply from 216.58.203.14: bytes=32 time=8ms TTL=119
Reply from 216.58.203.14: bytes=32 time=12ms TTL=119
Reply from 216.58.203.14: bytes=32 time=25ms TTL=119

Ping statistics for 216.58.203.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 25ms, Average = 13ms
```

Tcpdump-



```
┌──(manasi㉿kali)-[~]
└─$ sudo tcpdump -c 10
[sudo] password for manasi:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:28:28.727639 IP 192.168.102.1.54542 > 239.255.255.250.1900: UDP, length 174
23:28:28.729659 IP 192.168.102.128.39776 > 192.168.102.2.domain: 50796+ PTR? 250.255.255.239.in-addr.arpa. (46)
23:28:28.740689 ARP, Request who-has 192.168.102.128 tell 192.168.102.2, length 46
23:28:28.740718 ARP, Reply 192.168.102.128 is-at 00:0c:29:d3:80:83 (oui Unknown), length 28
23:28:28.741151 IP 192.168.102.2.domain > 192.168.102.128.39776: 50796 NXDomain 0/1/0 (103)
23:28:28.741641 IP 192.168.102.128.53516 > 192.168.102.2.domain: 29840+ PTR? 1.102.168.192.in-addr.arpa. (44)
23:28:28.756230 IP 192.168.102.2.domain > 192.168.102.128.53516: 29840 NXDomain 0/1/0 (121)
23:28:28.756838 IP 192.168.102.128.52083 > 192.168.102.2.domain: 53916+ PTR? 2.102.168.192.in-addr.arpa. (44)
23:28:28.768487 IP 192.168.102.2.domain > 192.168.102.128.52083: 53916 NXDomain 0/1/0 (121)
23:28:28.768864 IP 192.168.102.128.58230 > 192.168.102.2.domain: 22051+ PTR? 128.102.168.192.in-addr.arpa. (46)
10 packets captured
11 packets received by filter
0 packets dropped by kernel
```

Dig-



```
┌──(manasi㉿kali)-[~]
└─$ dig google.com

; <<>> DiG 9.16.11-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; —»HEADER«— opcode: QUERY, status: NOERROR, id: 9601
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             5       IN      A       142.250.77.46

;; AUTHORITY SECTION:
google.com.             5       IN      NS      ns2.google.com.
google.com.             5       IN      NS      ns1.google.com.
google.com.             5       IN      NS      ns3.google.com.
google.com.             5       IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.         5       IN      A       216.239.34.10
ns2.google.com.         5       IN      AAAA    2001:4860:4802:34::a
ns1.google.com.         5       IN      A       216.239.32.10
ns1.google.com.         5       IN      AAAA    2001:4860:4802:32::a
ns3.google.com.         5       IN      A       216.239.36.10
ns3.google.com.         5       IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         5       IN      A       216.239.38.10
ns4.google.com.         5       IN      AAAA    2001:4860:4802:38::a

;; Query time: 19 msec
;; SERVER: 192.168.102.2#53(192.168.102.2)
;; WHEN: Mon Feb 22 23:35:15 IST 2021
;; MSG SIZE  rcvd: 303
```

## Conclusion

Hence , we have understood and implemented basic networking commands.