**CN LAB**

**EXPERIMENT 01**

Name: Sreekesh Iyer Class/Roll No: D10A/24

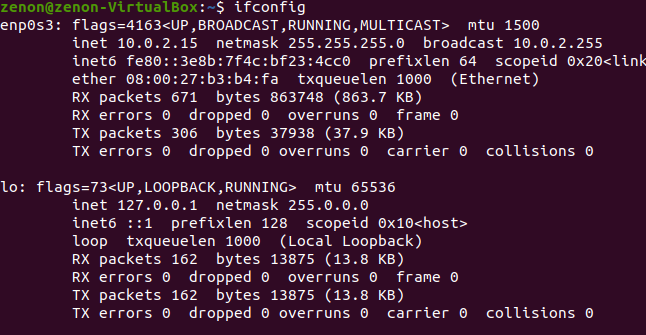
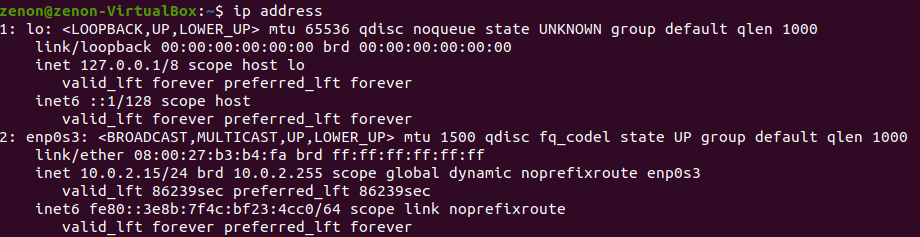
**Aim:** Understanding Basic Networking Commands

**Theory:**

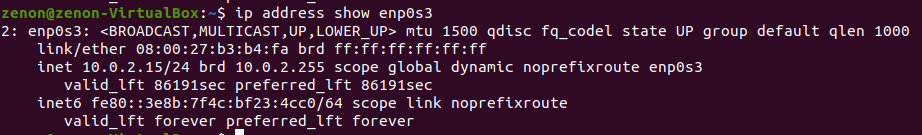
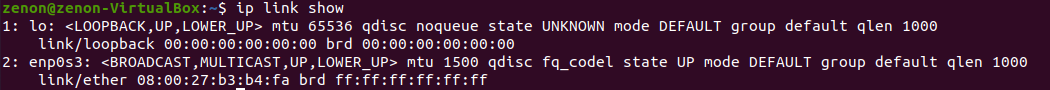
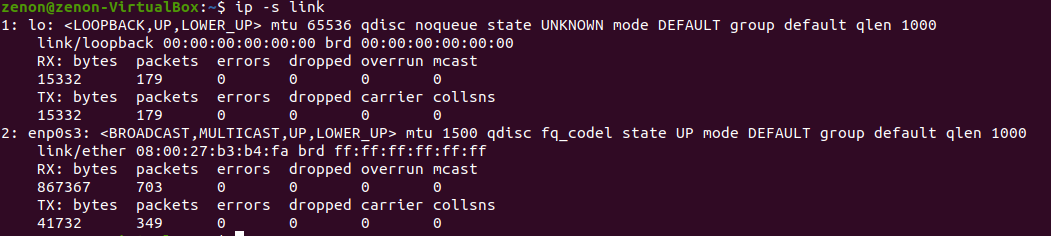
To understand different aspects of networking, Linux has in-built commands in its shell to show different properties of a network, network(s) you are connected to and how data is transferred.

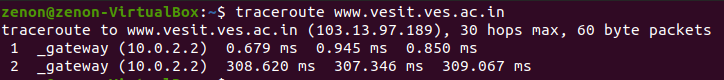
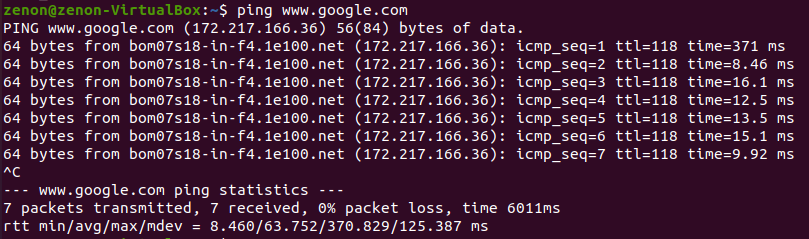
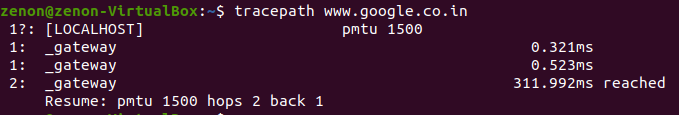
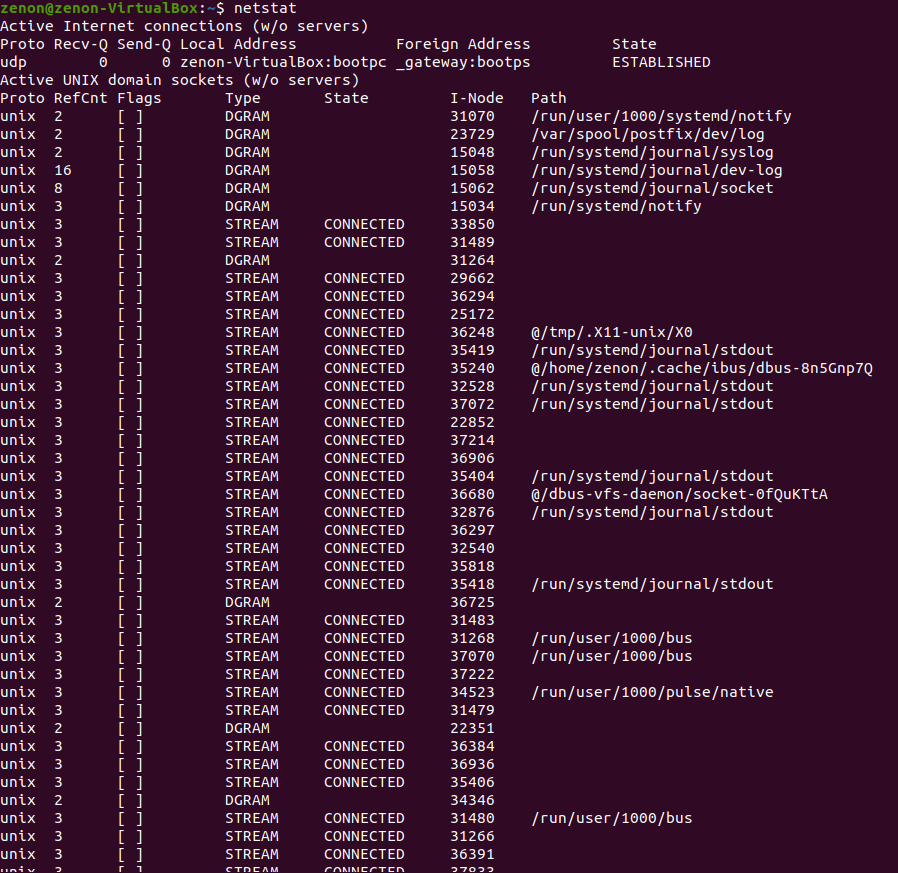
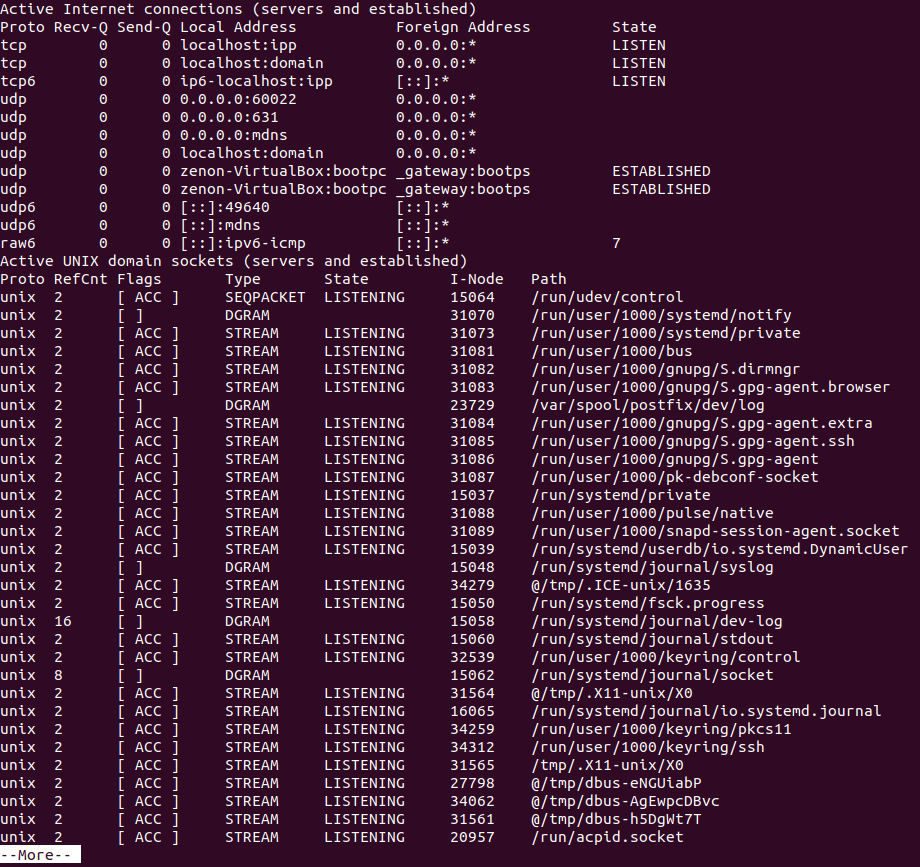
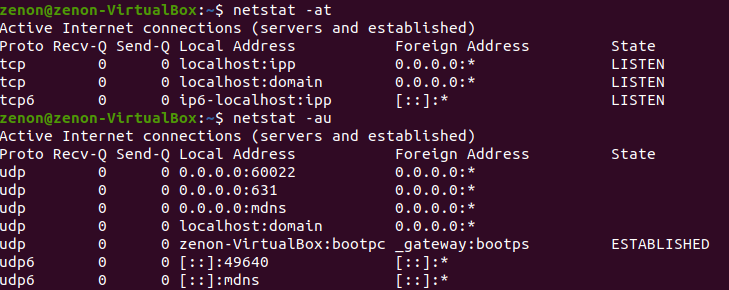
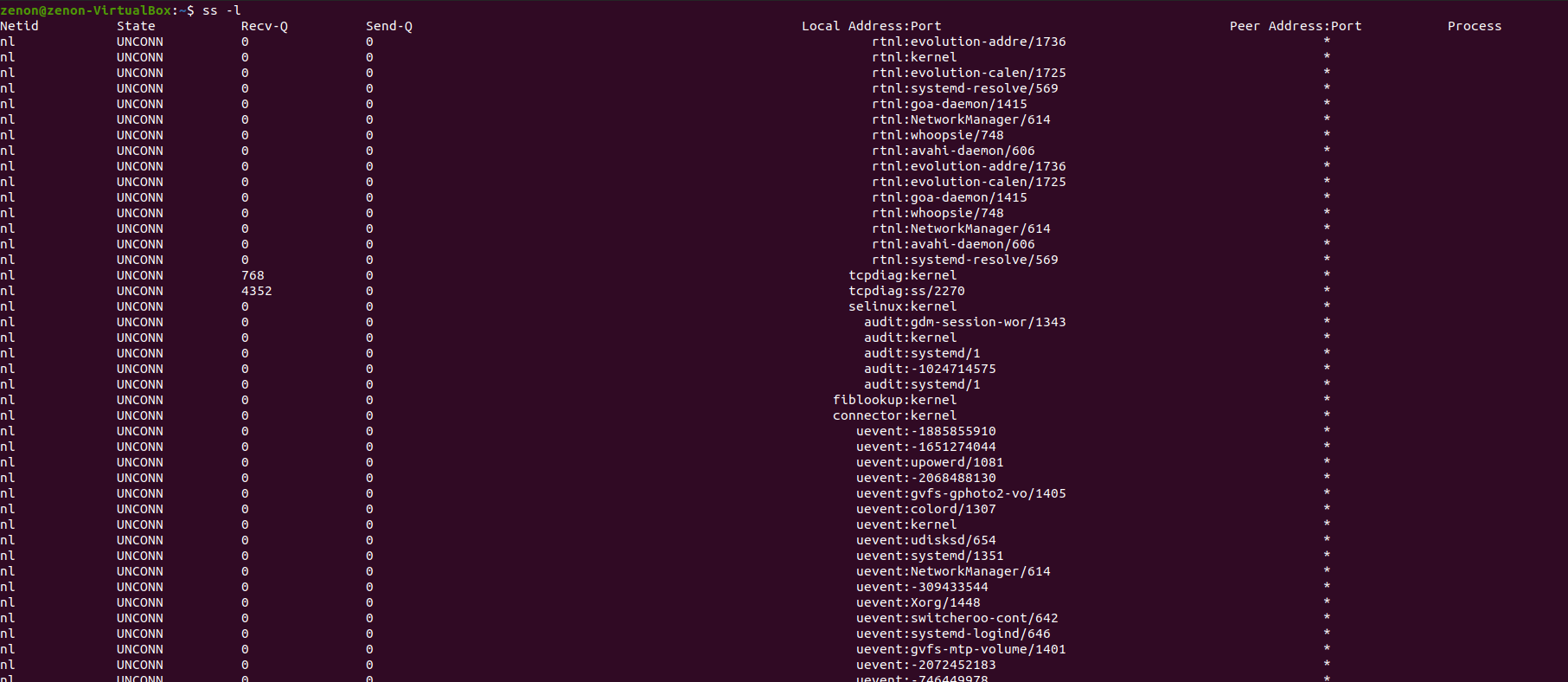
These networking commands might be needed/are generally used for network configuration, network administration and troubleshooting.

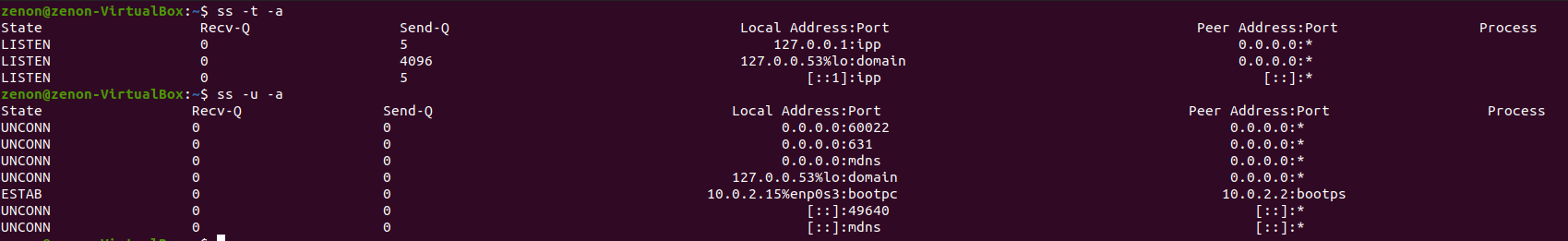
Listed below are a few examples of networking commands in Linux along with their explanations.

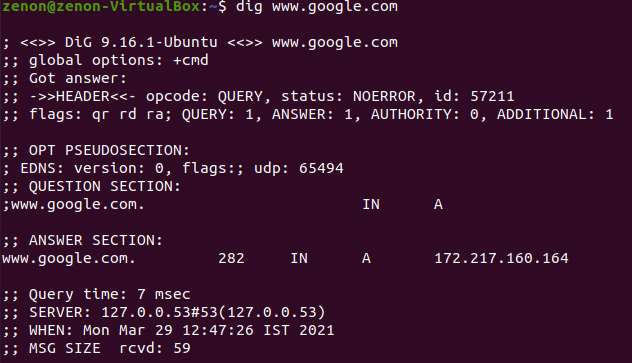
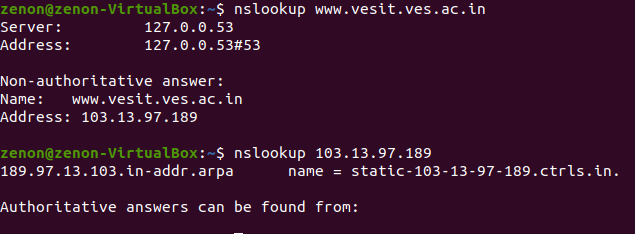
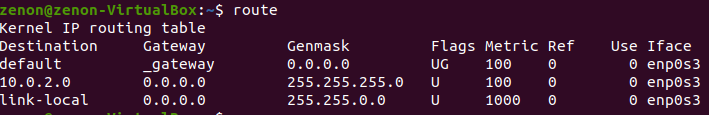
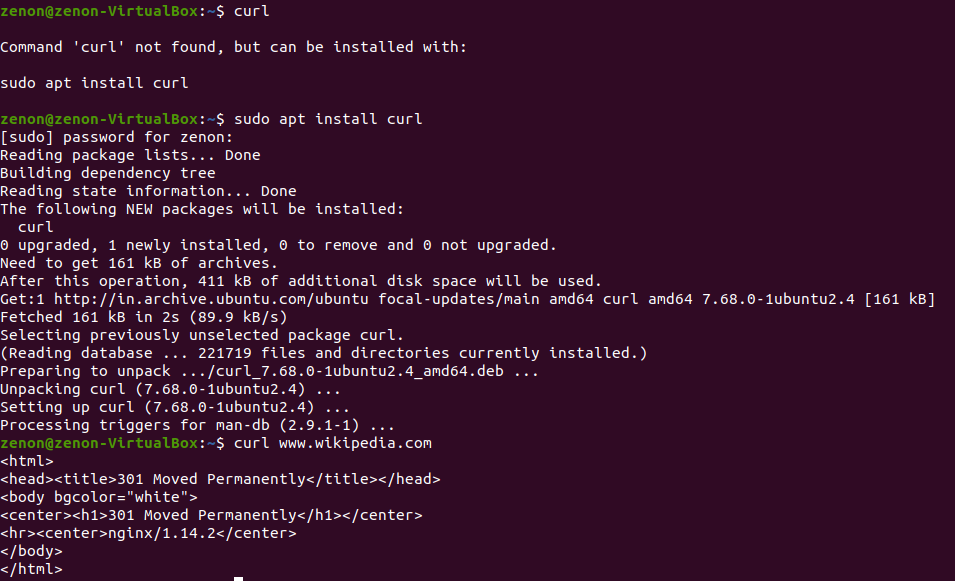
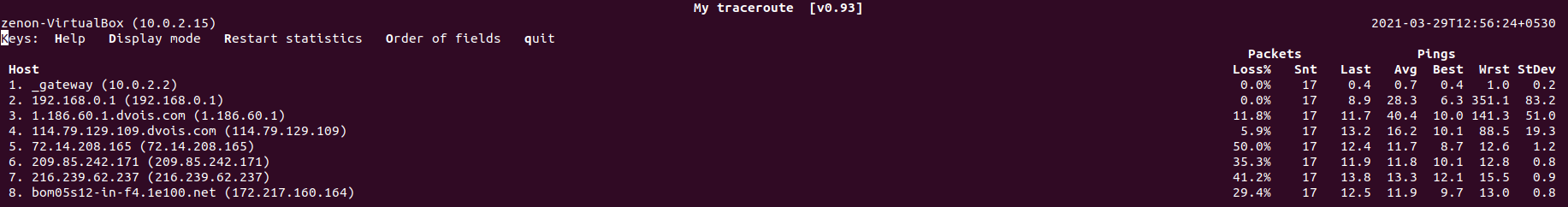
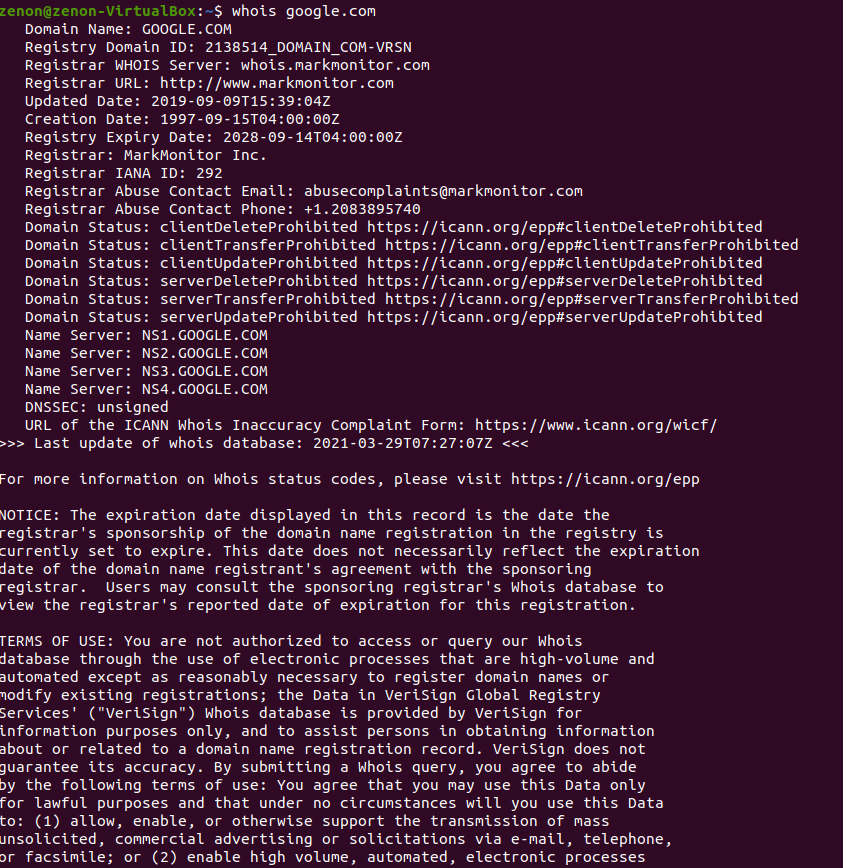
1. **ifconfig**  
     
     
   ifconfig is the command used for retrieving details about all present and working network interfaces of a machine. It’s a straight forward syntax, *ifconfig* with no arguments. The output looks like this, it shows the primary interface in use, in my case, is the virtual NAT network (a virtual Ethernet interface). On the left corner is the interface name and alongside is its information which includes IPv4 and IPv6 addresses and also the broadcast address and the subnet mask. Along with the main interface there is also the same information presented for the loopback network in *lo*.   
     
   The Internet Protocol (IP) specifies a loopback network with the (IPv4) address 127.0.0.0/8. Most IP implementations support a loopback interface (lo0) to represent the loopback facility. Any traffic that a computer program sends on the loopback network is addressed to the same computer. The most commonly used IP address on the loopback network is 127.0.0.1 for IPv4 and ::1 for IPv6. The standard domain name for the address is localhost.
2. **ip**  
     
     
   The ip command is a Linux net-tool for system and network administrators. IP stands for Internet Protocol and as the name suggests, the tool is used for configuring network interfaces.

Older Linux distributions used the ifconfig command, which operates similarly. However, ifconfig has a limited range of capabilities compared to the ip command.

  
  
  
  
  
The argument show along with ip command is used to see link-layer information of devices. Paired with interface name, this command can be used to see link-layer information of an individual NIC.   
  
  
  
The command **ip -s link** can be used to see the statistics for all network interfaces which includes details such as transferred and dropped packets, errors if any, etc.

1. **traceroute**  
     
     
   traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. Below image depicts how traceroute command is used to reach the Google(172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.  
   The first column corresponds to the hop count. The second column represents the address of that hop and after that, you see three space-separated time in milliseconds. traceroute command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop.  
   *Syntax:* **traceroute [options] host\_address [pathLength]**
2. **ping**   
     
     
   The ping command is a simple utility used to check whether a network is available and if a host is reachable. With this command, we can test if a server is up and running. It also helps in troubleshooting various connectivity issues.   
     
   When you try to “ping” a remote host, your machine starts sending ICMP echo requests and waits for a response. If the connection is established, you receive an echo reply for every request. The output for the ping command contains the amount of time it takes for every packet to reach its destination and return. The terminal keeps printing the responses until interrupted. After every session, there are a few lines with ping statistics.
3. **tracepath**  
     
     
   The tracepath command in Linux is used to trace a path to destination discovering MTU along this path. It uses a UDP port or some random port. It is similar to traceroute, but it does not require superuser privileges and has no fancy options. tracepath6 is a good replacement for traceroute6 and a classic example of the application of Linux error queues.  
     
   The tracepath command without any options prints the general syntax of the command along with the various options that can be used with the tracepath command as well as gives a brief description about each option.  
     
   The tracepath command with a set destination provides the path through which packets have been sent, as you can see, there were 2 hops made and the destination was reached in approximately 312 ms.
4. **netstat**   
     
     
   Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.  
     
     
     
     
   **netstat -a | more**  
     
   The command with -a|more arguments shows all listening and non-listening state sockets with the *More* Button to generate a rather organized result.   
     
     
   -at is used for listing all tcp ports while -au is used for listing all udp ports.
5. **ss**   
     
     
   The ss command is a tool used to dump socket statistics and displays information in similar fashion (although simpler and faster) to netstat. The ss command can also display even more TCP and state information than most other tools. Because ss is the new netstat, we’re going to take a look at how to make use of this tool so that you can more easily gain information about your Linux machine and what’s going on with network connections.  
     
   The command *ss - l* is used to list all listening sockets.

The ss command-line utility can display stats for the likes of PACKET, TCP, UDP, DCCP, RAW, and Unix domain sockets. The replacement for netstat is easier to use (compare the man pages to get an immediate idea of how much easier ss is). With ss, you get very detailed information about how your Linux machine is communicating with other machines, networks, and services; details about network connections, networking protocol statistics, and Linux socket connections. With this information in hand, you can much more easily troubleshoot various networking issues.  
  
  
  
*ss -t -a* is used to list all tcp sockets while *ss -u -a* is used to list all udp sockets.

1. **dig**   
     
     
   The dig command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data about Domain Name Servers. The dig command is helpful for diagnosing DNS problems, but is also used to display DNS information.  
   The Answer Section:  
   The first column lists the name of the server that was queried. The second column is *Time to Live*, a set time frame after which the record is refreshed. The third column shows the class of the query, in this case, *IN* stands for Internet. The fourth column shows the type of query, in this case, *A* stands for Address record. The final column displays the IP address associated with the domain name.
2. **nslookup**   
     
     
   Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from a DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.  
     
   nslookup followed by the domain name will display the “A Record” (IP Address) of the domain. Use this command to find the address record for a domain. It queries domain name servers and gets the details.  
   You can also do the reverse DNS look-up by providing the IP Address as argument to nslookup.
3. **route**   
     
     
   route Command is used when you have to work with the Kernel IP routing table. It shows the destination IP, the gateway, the subnet along with user id and the name of the interface in use.
4. **host**   
     
     
   host command in the 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.  
   host along with IP address will display the domain details of the specified IP Address.
5. **arp**   
     
     
   arp command manipulates the System’s ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).
6. **hostname**   
     
   It displays the name of the host machine.
7. **curl/wget**   
     
     
   curl is a command line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE). curl is powered by Libcurl. This tool is preferred for automation, since it is designed to work without user interaction. curl can transfer multiple files at once.
8. **mtr**  
     
     
   Mtr(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.  
     
   Mtr is basically a version of traceroute which reports in real-time. Just like traceroute, it shows data of packets and pings.
9. **whois**   
     
     
   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.  
     
   Most modern versions of whois try to guess the right server to ask for the specified object. If no guess can be made, whois will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.