Name: Shreya Chawale
Roll No. 22

Date: 26/01/2024

Lab Assignment No. 1

Aim: To get familiar with the basic network administration commands.

Lab Outcome Attained: Execute and evaluate network administration commands and demonstrate their use in different network scenarios.

Theory & Screenshots :

Windows runnable commands:

1)ipconfig/ifconfig

The ipconfig command is used to display information about your network configuration and refresh DHCP and DNS Settings. By default, the ipconfig command displays your IP Address, Subnet Mask, and default gateway.

-ipconfig /all

the /all parameter we used above will list all of your network adapters' configuration information.

-ipconfig /allcompartments

the /allcompartments will output the same information as the ipconfig command without any parameters.

-ipconfig /displaydns

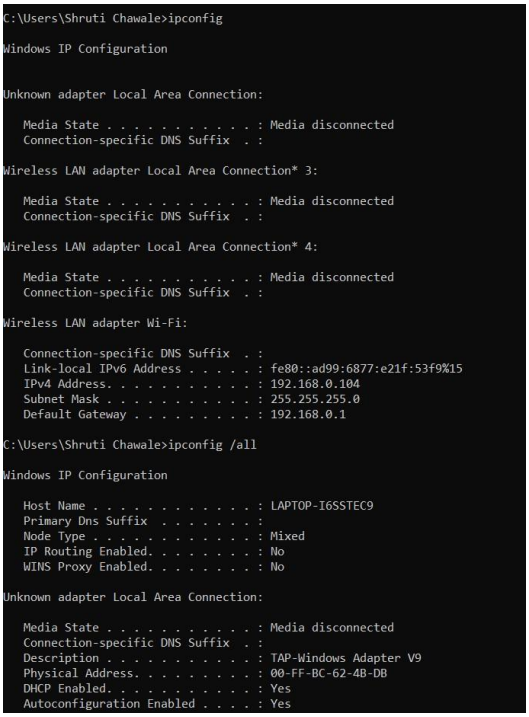
This /displaydns parameter shows the DNS resolver cache of your system. The cache cuts down on network traffic since it keeps track of IP addresses and website names you have already visited.

-ipconfig /flushdns

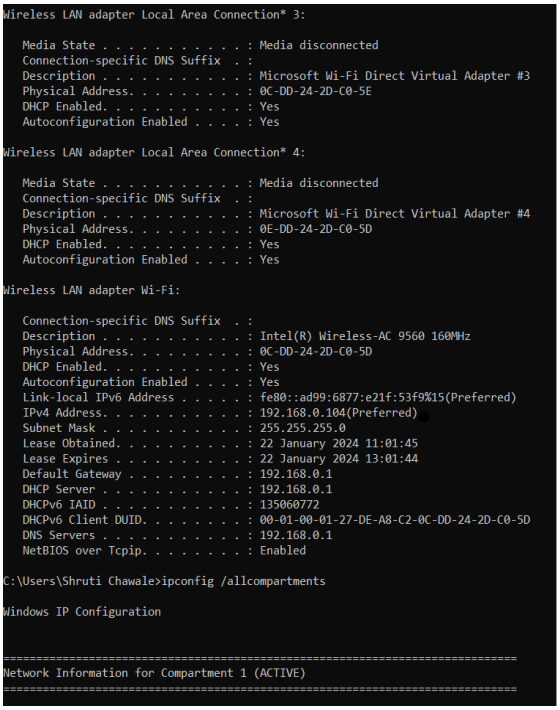
The /flushdns parameter will flush the DNS resolver cache. This can be useful when you are troubleshooting or when you want to get rid of defective or obsolete DNS records. The cache will be repopulated as you browse the Internet or during normal system activity.

-ipconfig /registerdns

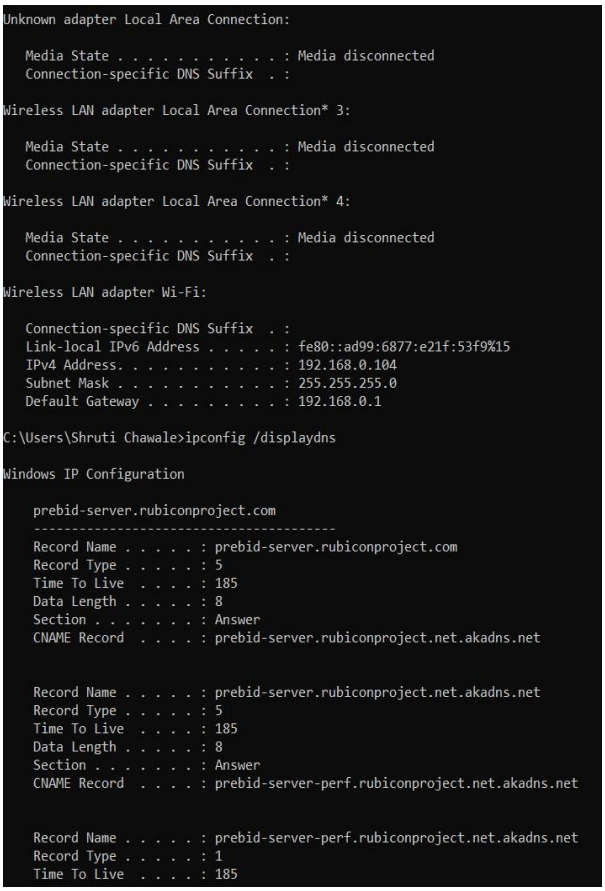
The /registerdns parameter registers (or refreshes) all DHCP leases and re-registers DNS names for all your system's network adapters.



```
C:\Users\Shruti Chawale>ipconfig

Windows IP Configuration


Unknown adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 4:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ad99:6877:e21f:53f9%15
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\Shruti Chawale>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-I6SSTEC9
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-BC-62-4B-DB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```



```
Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : 0C-DD-24-2D-C0-5E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : 0E-DD-24-2D-C0-5D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 0C-DD-24-2D-C0-5D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ad99:6877:e21f:53f9%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 22 January 2024 11:01:45
   Lease Expires . . . . . . . . . . : 22 January 2024 13:01:44
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 135060772
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-DE-A8-C2-0C-DD-24-2D-C0-5D
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Shruti Chawale>ipconfig /allcompartments

Windows IP Configuration


================================================================================
Network Information for Compartment 1 (ACTIVE)
================================================================================
```



```
Unknown adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 4:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ad99:6877:e21f:53f9%15
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\Shruti Chawale>ipconfig /displaydns

Windows IP Configuration

    prebid-server.rubiconproject.com
    ----------------------------------------
    Record Name . . . . . : prebid-server.rubiconproject.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 185
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : prebid-server.rubiconproject.net.akadns.net


    Record Name . . . . . : prebid-server.rubiconproject.net.akadns.net
    Record Type . . . . . : 5
    Time To Live  . . . . : 185
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : prebid-server-perf.rubiconproject.net.akadns.net


    Record Name . . . . . : prebid-server-perf.rubiconproject.net.akadns.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 185
```

```
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 69.173.158.92


    mssplus.mcafee.com
    ----------------------------------------
    No records of type AAAA


    mssplus.mcafee.com
    ----------------------------------------
    Record Name . . . . . : mssplus.mcafee.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 0
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 0.0.0.1


    1.0.0.0.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 1.0.0.0.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 0
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : mssplus.mcafee.com



C:\Users\Shruti Chawale>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Shruti Chawale>ipconfig /registerdns
The requested operation requires elevation.
```

2)ip

DOS/Windows IP commands are used to perform several tasks, like assigning an Internet Protocol (IP) address to a network interface or configuring network interface parameters.

This is used in linux

3)traceroute

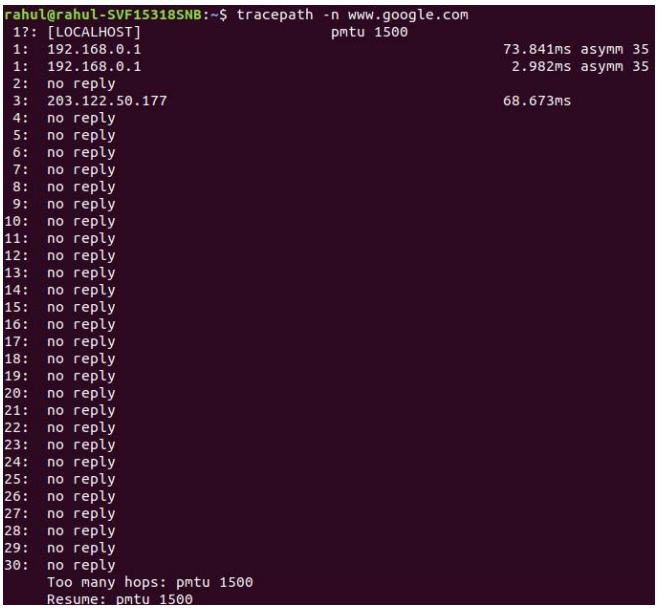
A traceroute provides a map of how data on the internet travels from its source to its destination. When you connect with a website, the data you get must travel across multiple devices and networks along the way, particularly routers.

Used on linux

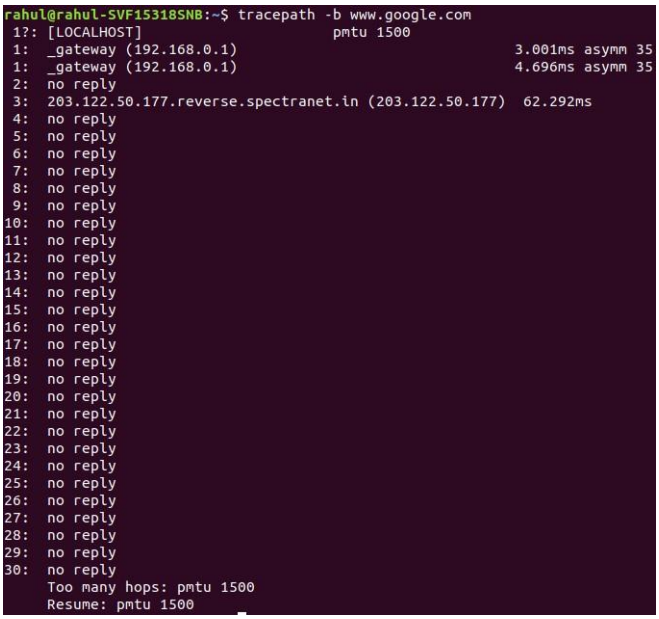
4)tracepath

Tracepath traces a path to a designated network address, reporting on the "time to live" or TTL lag and maximum transmission units (MTU) along the way.

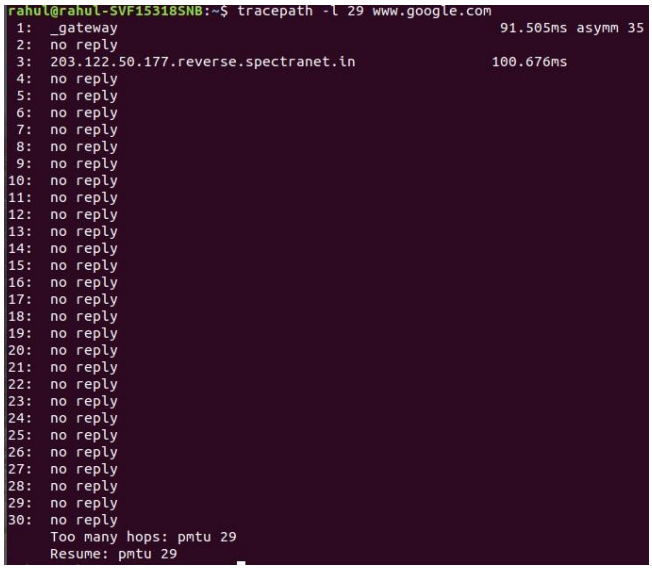
-tracepath -n www.google.com



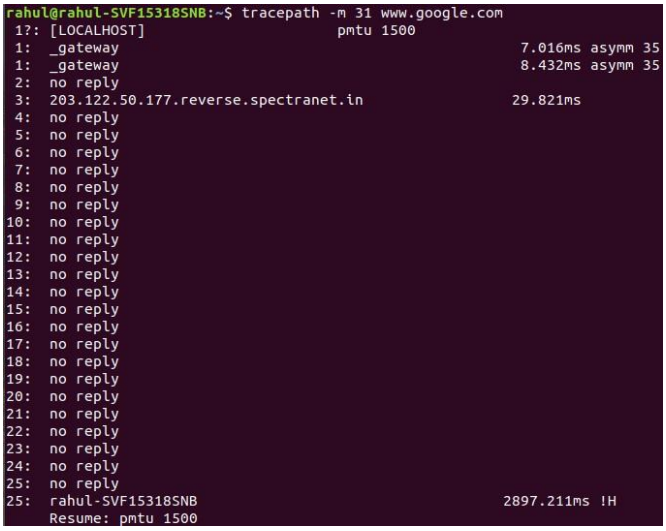
-tracepath -b www.google.com



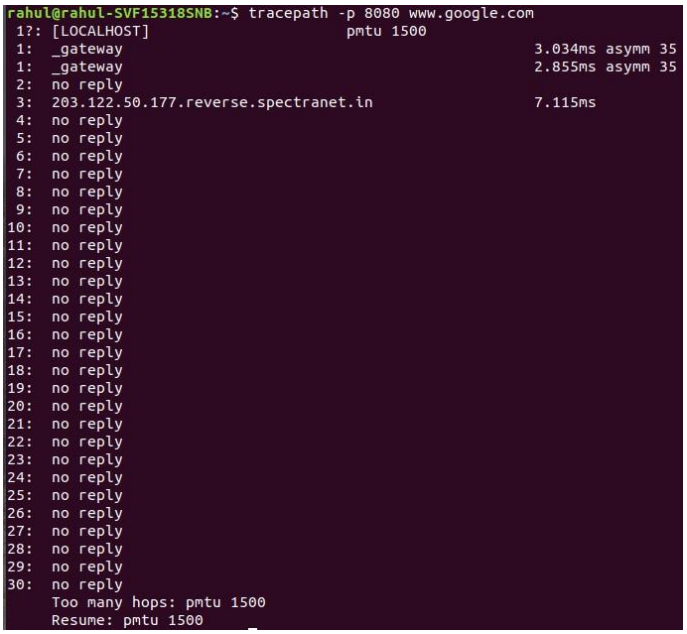
-tracepath -l



-tracepath -m



-tracepath -p



Source: geeksforgeeks

5)ping

ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.

-ping -t

Using this option will ping the target until you force it to stop by using Ctrl+C.

-ping -a

This ping command option will resolve, if possible, the hostname of an IP address target.

-ping -n count

Number of echo requests to send.

-ping -l size

Send buffer size.

-ping -f

Set Don't Fragment flag in packet (IPv4-only).

```
C:\Users\Shruti Chawale>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\Users\Shruti Chawale>ping -t
IP address must be specified.

C:\Users\Shruti Chawale>ping -t 192.168.1.138

Pinging 192.168.1.138 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.138:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Shruti Chawale>ping -a 192.168.1.138

Pinging 192.168.1.138 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.138:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Shruti Chawale>ping -n count
Bad value for option -n, valid range is from 1 to 4294967295.

C:\Users\Shruti Chawale>ping -n 30
IP address must be specified.

C:\Users\Shruti Chawale>ping -n 30 192.168.1.138

Pinging 192.168.1.138 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.138:
    Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Control-C
^C
C:\Users\Shruti Chawale>ping -l 20 192.168.1.138

Pinging 192.168.1.138 with 20 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.138:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Shruti Chawale>ping -f 192.168.1.138

Pinging 192.168.1.138 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

6)netstat

NetStat can validate the various network data paths on Windows, testing native, synthetic, and hardware offloaded (RDMA) data paths for issues with: Connectivity.

-netstat -a

This switch displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to.

-netstat -b

This netstat switch is very similar to the -o switch listed below, but instead of displaying the PID, will display the process's actual file name.

-netstat -e

Use this switch with the netstat command to show statistics about your network connection. This data includes bytes, unicast packets, non-unicast packets, discards, errors, and unknown protocols received and sent since the connection was established.

-netstat -f

The -f switch will force the netstat command to display the Fully Qualified Domain Name (FQDN) for each foreign IP addresses when possible.

-netstat -n

Use the -n switch to prevent netstat from attempting to determine host names for foreign IP addresses.

```
C:\Users\Shruti Chawale>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49666        LAPTOP-I6SSTEC9:57104  ESTABLISHED
  TCP    127.0.0.1:49672        LAPTOP-I6SSTEC9:49673  ESTABLISHED
  TCP    127.0.0.1:49673        LAPTOP-I6SSTEC9:49672  ESTABLISHED
  TCP    127.0.0.1:49674        LAPTOP-I6SSTEC9:49675  ESTABLISHED
  TCP    127.0.0.1:49675        LAPTOP-I6SSTEC9:49674  ESTABLISHED
  TCP    127.0.0.1:57104        LAPTOP-I6SSTEC9:49666  ESTABLISHED
  TCP    192.168.0.104:59881    20.198.119.84:https    ESTABLISHED
  TCP    192.168.0.104:59901    si-in-f188:5228        ESTABLISHED
  TCP    192.168.0.104:60716    69.173.158.68:https    ESTABLISHED
  TCP    192.168.0.104:60717    69.173.158.67:https    ESTABLISHED
  TCP    192.168.0.104:60869    server-18-172-218-117:https  ESTABLISHED
  TCP    192.168.0.104:60890    ec2-13-126-70-76:https  ESTABLISHED
  TCP    192.168.0.104:60891    a23-201-200-86:https   ESTABLISHED
  TCP    192.168.0.104:60893    a96-6-35-129:https     ESTABLISHED
  TCP    192.168.0.104:60894    a96-6-35-129:https     ESTABLISHED
  TCP    192.168.0.104:60895    server-108-158-61-40:https  ESTABLISHED
  TCP    192.168.0.104:60896    a104-120-93-64:https   ESTABLISHED
  TCP    192.168.0.104:60898    server-108-158-61-106:https  ESTABLISHED
  TCP    192.168.0.104:60899    server-108-158-61-106:https  ESTABLISHED
  TCP    192.168.0.104:60900    server-108-158-61-73:https  ESTABLISHED
  TCP    192.168.0.104:60901    a104-120-93-64:https   ESTABLISHED
  TCP    192.168.0.104:60912    172.67.5.200:https     ESTABLISHED
  TCP    192.168.0.104:60913    199.232.254.137:https  ESTABLISHED
  TCP    192.168.0.104:60914    104.18.38.76:https     TIME_WAIT
  TCP    192.168.0.104:60915    server-108-159-58-51:https  TIME_WAIT
  TCP    192.168.0.104:60917    server-18-172-60-30:https  ESTABLISHED
  TCP    192.168.0.104:60920    server-18-67-195-40:https  ESTABLISHED
  TCP    192.168.0.104:60921    52.46.151.131:https    ESTABLISHED
  TCP    192.168.0.104:60926    67.199.150.87:https    ESTABLISHED
  TCP    192.168.0.104:60931    bom07s16-in-f1:https   ESTABLISHED
  TCP    192.168.0.104:60932    server-18-172-78-28:https  ESTABLISHED
  TCP    192.168.0.104:60933    server-18-172-64-39:https  ESTABLISHED
  TCP    192.168.0.104:60934    server-108-159-61-85:https  ESTABLISHED
  TCP    192.168.0.104:60935    8:https                TIME_WAIT
^C
C:\Users\Shruti Chawale>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:1593           LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:6646           LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:33060          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:49669          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:49682          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    0.0.0.0:50128          LAPTOP-I6SSTEC9:0      LISTENING
  TCP    127.0.0.1:5939         LAPTOP-I6SSTEC9:0      LISTENING
  TCP    127.0.0.1:27017        LAPTOP-I6SSTEC9:0      LISTENING
  TCP    127.0.0.1:49666        LAPTOP-I6SSTEC9:57104  ESTABLISHED
  TCP    127.0.0.1:49672        LAPTOP-I6SSTEC9:49673  ESTABLISHED
  TCP    127.0.0.1:49673        LAPTOP-I6SSTEC9:49672  ESTABLISHED
  TCP    127.0.0.1:49674        LAPTOP-I6SSTEC9:49675  ESTABLISHED
  TCP    127.0.0.1:49675        LAPTOP-I6SSTEC9:49674  ESTABLISHED
  TCP    127.0.0.1:49790        LAPTOP-I6SSTEC9:0      LISTENING
  TCP    127.0.0.1:56742        LAPTOP-I6SSTEC9:0      LISTENING
  TCP    127.0.0.1:57104        LAPTOP-I6SSTEC9:49666  ESTABLISHED
  TCP    192.168.0.104:139      LAPTOP-I6SSTEC9:0      LISTENING
^C
C:\Users\Shruti Chawale>netstat -b
The requested operation requires elevation.

C:\Users\Shruti Chawale>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    2891013732      2439318258
Unicast packets            59863242        20102388
Non-unicast packets         1043028           80568
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\Users\Shruti Chawale>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49666        LAPTOP-I6SSTEC9:57104  ESTABLISHED
  TCP    127.0.0.1:49672        LAPTOP-I6SSTEC9:49673  ESTABLISHED
  TCP    127.0.0.1:49673        LAPTOP-I6SSTEC9:49672  ESTABLISHED
  TCP    127.0.0.1:49674        LAPTOP-I6SSTEC9:49675  ESTABLISHED
  TCP    127.0.0.1:49675        LAPTOP-I6SSTEC9:49674  ESTABLISHED
  TCP    127.0.0.1:57104        LAPTOP-I6SSTEC9:49666  ESTABLISHED
```

```
C:\Users\Shruti Chawale>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49666        127.0.0.1:57104        ESTABLISHED
  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    127.0.0.1:57104        127.0.0.1:49666        ESTABLISHED
  TCP    192.168.0.104:59881    20.198.119.84:443      ESTABLISHED
  TCP    192.168.0.104:59901    172.217.194.188:5228   ESTABLISHED
  TCP    192.168.0.104:60716    69.173.158.68:443      ESTABLISHED
  TCP    192.168.0.104:60717    69.173.158.67:443      ESTABLISHED
  TCP    192.168.0.104:60869    18.172.218.117:443     ESTABLISHED
  TCP    192.168.0.104:60890    13.126.70.76:443       ESTABLISHED
  TCP    192.168.0.104:60891    23.201.200.86:443      ESTABLISHED
  TCP    192.168.0.104:60893    96.6.35.129:443        ESTABLISHED
  TCP    192.168.0.104:60894    96.6.35.129:443        ESTABLISHED
  TCP    192.168.0.104:60896    104.120.93.64:443      ESTABLISHED
  TCP    192.168.0.104:60901    104.120.93.64:443      ESTABLISHED
  TCP    192.168.0.104:60912    172.67.5.200:443       ESTABLISHED
  TCP    192.168.0.104:60913    199.232.254.137:443    ESTABLISHED
  TCP    192.168.0.104:60921    52.46.151.131:443      ESTABLISHED
  TCP    192.168.0.104:60926    67.199.150.87:443      ESTABLISHED
  TCP    192.168.0.104:60931    172.217.160.193:443    TIME_WAIT
  TCP    192.168.0.104:60937    104.26.3.116:443       ESTABLISHED
  TCP    192.168.0.104:60942    199.232.254.114:443    ESTABLISHED
  TCP    192.168.0.104:60945    23.212.255.169:443     ESTABLISHED
  TCP    192.168.0.104:60948    151.101.2.114:443      ESTABLISHED
  TCP    192.168.0.104:60950    151.101.2.114:443      ESTABLISHED
  TCP    192.168.0.104:60953    69.173.158.64:443      ESTABLISHED
  TCP    192.168.0.104:60954    104.17.219.204:443     ESTABLISHED
  TCP    192.168.0.104:60958    151.101.2.49:443       ESTABLISHED
  TCP    192.168.0.104:60961    69.173.158.64:443      ESTABLISHED
  TCP    192.168.0.104:60962    69.173.158.64:443      ESTABLISHED
  TCP    192.168.0.104:60964    69.173.158.64:443      ESTABLISHED
  TCP    192.168.0.104:60965    69.173.158.64:443      ESTABLISHED
  TCP    192.168.0.104:60966    69.173.158.64:443      ESTABLISHED
  TCP    192.168.0.104:60968    34.107.140.113:443     ESTABLISHED
  TCP    192.168.0.104:60972    57.128.112.22:443      ESTABLISHED
  TCP    192.168.0.104:60974    34.107.148.139:443     ESTABLISHED
  TCP    192.168.0.104:60981    172.217.174.67:443     ESTABLISHED
  TCP    192.168.0.104:60984    216.58.196.67:443      ESTABLISHED
  TCP    192.168.0.104:60985    20.42.65.88:443        ESTABLISHED
  TCP    192.168.0.104:60986    142.250.70.110:443     ESTABLISHED
  TCP    192.168.0.104:60988    104.91.32.229:443      ESTABLISHED
```

7)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.

```
~ $ ss
Netid  State      Recv-Q Send-Q Local Address:Port    Peer Address:Port
u_seq  ESTAB      0      0      @00002b 40545          * 40546
u_seq  ESTAB      0      0      @00002a 40543          * 40544
u_str  ESTAB      0      0       * 47336               * 47335
u_str  ESTAB      0      0       * 37615               * 37616
u_str  ESTAB      0      0       * 37263               * 36819
u_str  ESTAB      0      0       * 37816               * 37817
u_str  ESTAB      0      0       * 40173               * 40174
u_str  ESTAB      0      0       * 38066               * 39294
```

-ss -a

List all listening and non-listening connections with.

```
~ $ ss -a
Netid  State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
nl     UNCONN     0      0      rtnl:avahi-daemon/911      *
nl     UNCONN     0      0      rtnl:1828717503            *
nl     UNCONN     0      0      rtnl:chrome/4111           *
nl     UNCONN     0      0      rtnl:vmnet-natd/1562       *
nl     UNCONN     0      0      rtnl:kernel                *
nl     UNCONN     0      0      rtnl:vmnet-bridge/1495     *
nl     UNCONN     0      0      rtnl:chrome/4058           *
nl     UNCONN     0      0      rtnl:dnsmasq/1170          *
```

-ss -l

To display only listening sockets, which are omitted by default.

```
~ $ ss -l
Netid  State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
nl     UNCONN     0      0      rtnl:avahi-daemon/911       *
nl     UNCONN     0      0      rtnl:1828717503             *
nl     UNCONN     0      0      rtnl:chrome/4111            *
nl     UNCONN     0      0      rtnl:vmnet-natd/1562        *
nl     UNCONN     0      0      rtnl:kernel                 *
nl     UNCONN     0      0      rtnl:vmnet-bridge/1495      *
nl     UNCONN     0      0      rtnl:chrome/4058            *
nl     UNCONN     0      0      rtnl:dnsmasq/1170           *
```

-ss -t

To list TCP connections, add the -t option to the ss command

```
~ $ ss -t
State      Recv-Q Send-Q   Local Address:Port                 Peer Address:Port
ESTAB      0      0        192.168.100.2:34494              108.177.126.188:5228
ESTAB      0      0        192.168.100.2:45618              142.250.184.150:https
ESTAB      0      0        192.168.100.2:39146                   52.85.7.80:https
```

-ss -at

Combine the options -a and -t with the ss command to output a list of all the TCP connections:

```
~ $ ss -at
State      Recv-Q Send-Q   Local Address:Port                 Peer Address:Port
LISTEN     0      80           127.0.0.1:mysql                       *:*
LISTEN     0      5            127.0.1.1:domain                      *:*
LISTEN     0      5            127.0.0.1:ipp                         *:*
ESTAB      0      0        192.168.100.2:34494              108.177.126.188:5228
ESTAB      0      0        192.168.100.2:45618              142.250.184.150:https
ESTAB      0      0        192.168.100.2:39146                   52.85.7.80:https
LISTEN     0      128             :::http                         :::*
LISTEN     0      5              ::1:ipp                          :::*
```

-ss -lt

Combine the options -l and -t with the ss command to list all listening TCP connections:

```
~ $ ss -lt
State      Recv-Q Send-Q   Local Address:Port                 Peer Address:Port
LISTEN     0      80           127.0.0.1:mysql                       *:*
LISTEN     0      5            127.0.1.1:domain                      *:*
LISTEN     0      5            127.0.0.1:ipp                         *:*
LISTEN     0      128             :::http                         :::*
LISTEN     0      5              ::1:ipp                          :::*
```

8)dig

The dig (domain information groper) command is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the queried name server(s).

-dig [hostname]

Returns any A record found within the queried hostname’s zone.

-dig [hostname] [record type]

Returns the records of that type found within the queried hostname’s zone. List of Record Types.

-dig [hostname] +short

Provides a terse answer, usually just an IP address.

-dig @[nameserver address hostname]

Queries the nameserver directly instead of your ISP's resolver.

-dig [hostname] +trace

Adding +trace instructs dig to resolve the query from the root nameserver downwards and to report the results from each query step.

9)nslookup

Nslookup is the name of a program that lets users enter a host name and find out the corresponding IP address or domain name system (DNS) record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address.

-nslookup -debug

Show debugging information.

-nslookup -timeout=[10]

Specify the time allowed for the server to respond.

-nslookup -type=a

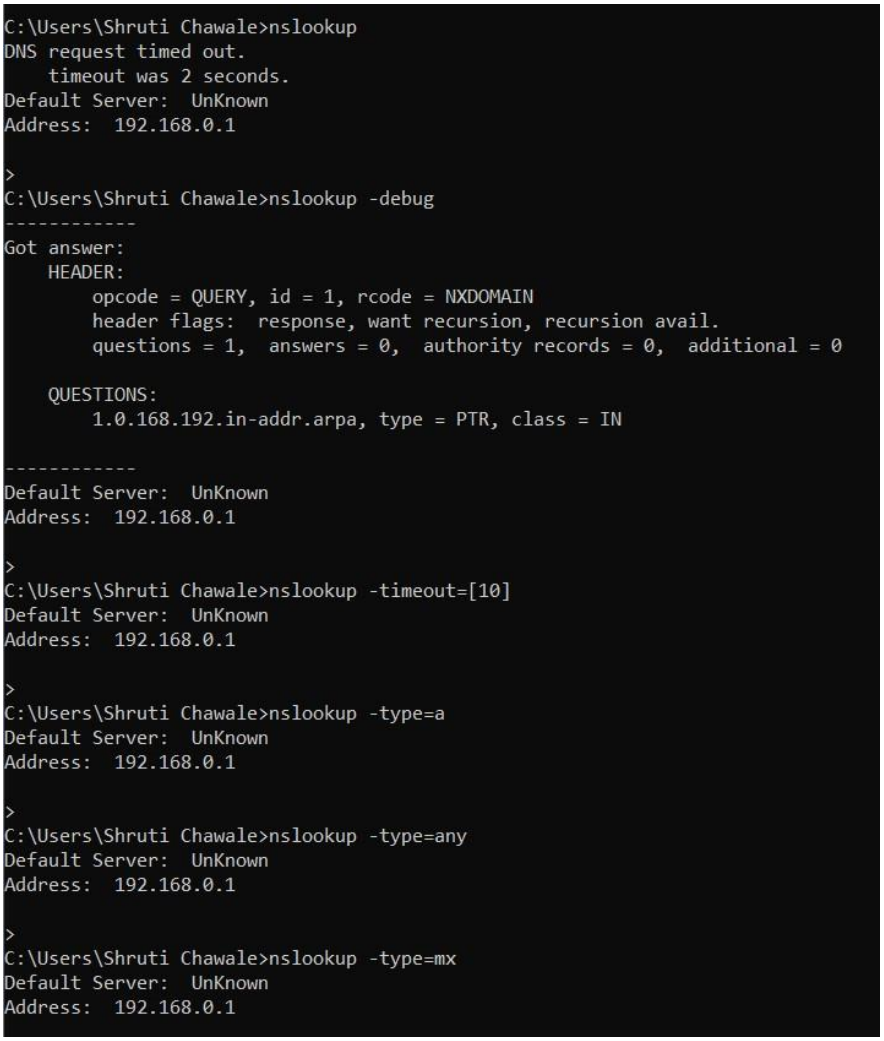
View information about the DNS A address records.

-nslookup -type=any

View all available records.

-nslookup -type=mx

View Mail Exchange server information.



10)route

The route command allows you to make manual entries into the network routing tables. The route command distinguishes between routes to hosts and routes to networks by interpreting the network address of the Destination variable, which can be specified either by symbolic name or numeric address.

-route -f

Purges all entries in the routing table that are not associated with network interfaces.

-route -n

Displays host and network names numerically, rather than symbolically, when reporting results of a flush or of any action in verbose mode.

-route -q

Specifies quiet mode and suppresses all output.

-route -v

Specifies verbose mode and prints additional details.

-route -net

Indicates that the Destination parameter should be interpreted as a network.

```
C:\Users\Shruti Chawale>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
```

```
Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32

C:\Users\Shruti Chawale>route -f
The requested operation requires elevation.

C:\Users\Shruti Chawale>route -f 192.168.1.168

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.
```

```
  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask
 Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.
```

```
C:\Users\Shruti Chawale>route -n 192.168.1.168

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
```

```
Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32

C:\Users\Shruti Chawale>route -q 192.168.1.168

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
```

```
All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask
 Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32

C:\Users\Shruti Chawale>route -v 192.168.1.168

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
```

```
 -p           When used with the ADD command, makes a route persistent across
              boots of the system. By default, routes are not preserved
              when the system is restarted. Ignored for all other commands,
              which always affect the appropriate persistent routes.

 -4           Force using IPv4.

 -6           Force using IPv6.

 command      One of these:
                PRINT     Prints  a route
                ADD       Adds    a route
                DELETE    Deletes a route
                CHANGE    Modifies an existing route
 destination  Specifies the host.
 MASK         Specifies that the next parameter is the 'netmask' value.
 netmask      Specifies a subnet mask value for this route entry.
              If not specified, it defaults to 255.255.255.255.
 gateway      Specifies gateway.
 interface    the interface number for the specified route.
 METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask)
 Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
```

```
 destination  Specifies the host.
 MASK         Specifies that the next parameter is the 'netmask' value.
 netmask      Specifies a subnet mask value for this route entry.
              If not specified, it defaults to 255.255.255.255.
 gateway      Specifies gateway.
 interface    the interface number for the specified route.
 METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mas
 Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32
```

11)host

The HOST command executes external commands at the operating system level. For a Windows operating system, for example, this is equivalent to running commands from a command prompt in a command window. No output is displayed in a command window.

-host ip address

This will display the domain details of the specified IP Address.

```
anshul@anshul-VirtualBox:~$ host 52.25.109.230
230.109.25.52.in-addr.arpa domain name pointer ec2-52-25-109-230.us-west-2.compute.amazonaws.com.
anshul@anshul-VirtualBox:~$
```

-host -a or -v

It used to specify the query type or enables the verbose output.

```
anshul@anshul-VirtualBox:~$ host -v geeksforgeeks.org
Trying "geeksforgeeks.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14557
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;geeksforgeeks.org.             IN      A

;; ANSWER SECTION:
geeksforgeeks.org.      8       IN      A       52.25.109.230

Received 51 bytes from 127.0.0.53#53 in 1 ms
Trying "geeksforgeeks.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11597
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;geeksforgeeks.org.             IN      AAAA

Received 35 bytes from 127.0.0.53#53 in 583 ms
Trying "geeksforgeeks.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43282
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;geeksforgeeks.org.             IN      MX

;; ANSWER SECTION:
geeksforgeeks.org.      278     IN      MX      5 alt2.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      5 alt1.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      10 alt4.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      10 alt3.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      1 aspmx.l.google.com.

Received 153 bytes from 127.0.0.53#53 in 3 ms
anshul@anshul-VirtualBox:~$
```

-host -t

It is used to specify the type of query.

```
anshul@anshul-VirtualBox:~$ host -t ns geeksforgeeks.org
geeksforgeeks.org name server ns-869.awsdns-44.net.
geeksforgeeks.org name server ns-245.awsdns-30.com.
geeksforgeeks.org name server ns-1569.awsdns-04.co.uk.
geeksforgeeks.org name server ns-1520.awsdns-62.org.
anshul@anshul-VirtualBox:~$
```

-host SOA geeksforgeeks.org

To print SOA record

```
anshul@anshul-VirtualBox:~$ host -t SOA geeksforgeeks.org
geeksforgeeks.org has SOA record ns-869.awsdns-44.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
anshul@anshul-VirtualBox:~$
```

-host -t txt geeksforgeeks.org

To print text records

Source: geeksforgeeks

12)arp

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

-arp -a

Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed.

-arp -g

Same as -a

-arp -v

Displays current ARP entries in verbose mode. All invalid entries and entries on the loopback interface will be shown.

-arp -d

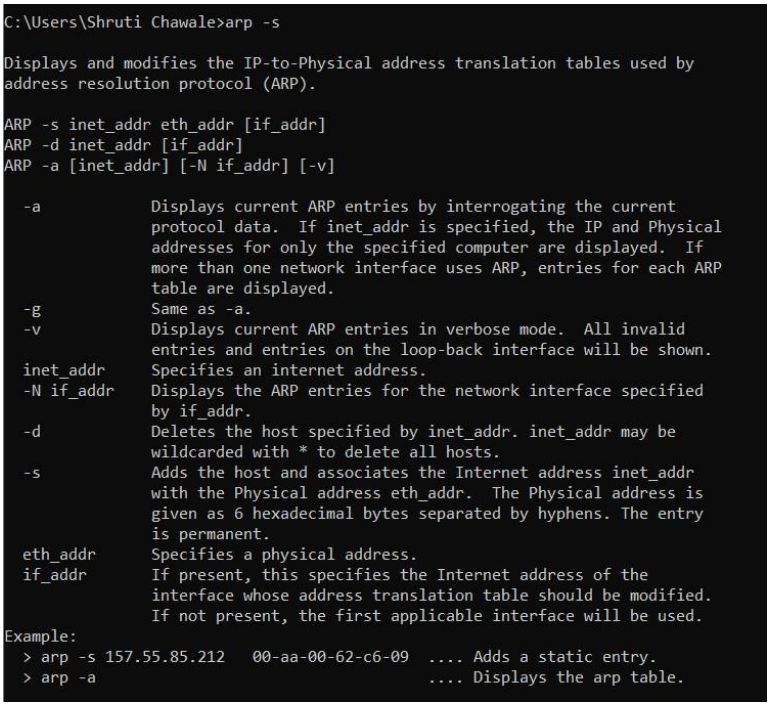
Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.

-arp -s

Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

```
C:\Users\Shruti Chawale>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.

C:\Users\Shruti Chawale>arp -a

Interface: 192.168.0.104 --- 0xf
  Internet Address      Physical Address      Type
  192.168.0.1           d8-07-b6-12-bd-fc     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Shruti Chawale>arp -g
```

```
Interface: 192.168.0.104 --- 0xf
  Internet Address      Physical Address      Type
  192.168.0.1           d8-07-b6-12-bd-fc     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Shruti Chawale>arp -v

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.

C:\Users\Shruti Chawale>arp -d
The ARP entry deletion failed: The requested operation requires elevation.
```



13)hostname

The /usr/bin/hostname command displays the name of the current host system. Only users with root user authority can set the host name. The mkdev command and the chdev commands also set the host name permanently.

-hostname -a

This option is used to get the alias name of the host system (if any). It will return an empty line if no alias name is set.

-hostname -A

This option is used to get all FQDNs (Fully Qualified Domain Name) of the host system. It enumerates all configured addresses on all network interfaces.

-hostname -b

Used to always set a hostname. Default name is used if none specified.

-hostname -d

This option is used to get the Domain if local domains are set. It will not return anything (not even a blank line) if no local domain is set.

-hostname -f

This option is used to get the Fully Qualified Domain Name (FQDN). It contains short hostname and DNS domain name.

```
C:\Users\Shruti Chawale>hostname
LAPTOP-I6SSTEC9

C:\Users\Shruti Chawale>hostname -a
sethostname: Use the Network Control Panel Applet to set hostname.
hostname -s is not supported.

C:\Users\Shruti Chawale>hostname -A
sethostname: Use the Network Control Panel Applet to set hostname.
hostname -s is not supported.

C:\Users\Shruti Chawale>hostname -b
sethostname: Use the Network Control Panel Applet to set hostname.
hostname -s is not supported.

C:\Users\Shruti Chawale>hostname -d
sethostname: Use the Network Control Panel Applet to set hostname.
hostname -s is not supported.

C:\Users\Shruti Chawale>hostname -s
sethostname: Use the Network Control Panel Applet to set hostname.
hostname -s is not supported.
```

14)curl

Client URL (cURL, pronounced "curl") is a command line tool that enables data exchange between a device and a server through a terminal. Using this command line interface (CLI), a user specifies a server URL (the location where they want to send a request) and the data they want to send to that server URL.

```
C:\Users\Shruti Chawale>curl --help
Usage: curl [options...] <url>
 -d, --data <data>          HTTP POST data
 -f, --fail                 Fail fast with no output on HTTP errors
 -h, --help <category>      Get help for commands
 -i, --include              Include protocol response headers in the output
 -o, --output <file>        Write to file instead of stdout
 -O, --remote-name          Write output to a file named as the remote file
 -s, --silent               Silent mode
 -T, --upload-file <file>   Transfer local FILE to destination
 -u, --user <user:password> Server user and password
 -A, --user-agent <name>    Send User-Agent <name> to server
 -v, --verbose              Make the operation more talkative
 -V, --version              Show version number and quit

This is not the full help, this menu is stripped into categories.
Use "--help category" to get an overview of all categories.
For all options use the manual or "--help all".
```

-curl [options/URLs]

The system outputs the HTML contents found on the URL provided after the curl command.

```
marko@test-main:~$ curl https://www.gnu.org/gnu/gnu.html
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<link rel="author" href="mailto:webmasters@gnu.org" />
<link rel="icon" type="image/png" href="/graphics/gnu-head-mini.png" />
<meta name="ICBM" content="42.355469,-71.058627" />
<link rel="stylesheet" type="text/css" href="/mini.css" media="handheld" />
<link rel="stylesheet" type="text/css" href="/layout.min.css" media="screen" />
<link rel="stylesheet" type="text/css" href="/print.min.css" media="print" />
```

-curl [url] > [local-file]

The progress bar shows how much of the file has been downloaded so far.

```
marko@test-main:~$ curl https://releases.ubuntu.com/20.04.3/ubuntu-20.04.3-desktop-amd6
4.iso >~/ubuntu.iso
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  8 2929M    8  236M    0     0  4521k      0  0:11:03  0:00:53  0:10:10 4216k
```

-curl –abstract-unix-socket <path>

Connect through abstract Unix socket instead through a network.

-curl –alt-svc <filename>

Enable alt-svc parser.

-curl -a

Append to the target file.

15)wget

Wget allows you to retrieve content and files from web servers using a command-line interface. The name “wget” comes from “World Wide Web” and “get”. Wget supports downloads via FTP, SFTP, HTTP, and HTTPS protocols. Wget is used by developers to automate file downloads.

```
sofija@sofija-VirtualBox: ~
File  Edit  View  Search  Terminal  Help
sofija@sofija-VirtualBox:~$ wget
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try `wget --help' for more options.
sofija@sofija-VirtualBox:~$
```

-wget -h

The output will show you an exhaustive list of all the wget command parameters.

-wget [URL]

To download a file from the web use.

-wget -O [file_name] [URL]

To download a file and save it under a specified name run.

-wget -P [wanted_directory] [URL]

By default wget downloads a file in the directory the user is in. To save the file in a different location, add the -P option.

-wget –limit-rate [wanted_speed] [URL]

You can set the download speed when downloading a big file, so it does not use the full available bandwidth. The download speed is defined in kilobytes (k) and megabytes (m). Use the command.

16)mtr

The name is a shorthand for My Traceroute, also known as Matt's Traceroute. mtr is a networking tool that combines ping and traceroute to diagnose a network. Instead of using both tools separately, we could use only mtr. The purpose of mtr is to analyze the network traffic hop-to-hop using ICMP packets.

-mtr <IP ADDRESS>/<HOSTNAME>

When you execute the command attaching an IP address or hostname, you will be redirected to its interface, which will be updated once per second or until you press the "q" button on your keyboard.

[root@server ~]# mtr -rw google.com

Start: Wed Apr 15 14:00:04 2020

HOST: server.hostname.com Loss% Snt Last Avg Best Wrst StDev

1.|-- 2a01:7e01::e6c7:22ff:fe1f:22c1 0.0% 10 0.9 1.3 0.9 2.0 0.0

2.|-- 2a01:7e01:b::1 0.0% 10 11.2 3.6 0.5 11.2 4.7

3.|-- de-cix.fra.google.com 0.0% 10 0.9 0.9 0.8 1.4 0.0

4.|-- 2001:4860:0:11df::1 0.0% 10 0.8 0.9 0.8 1.0 0.0

5.|-- 2001:4860:0:1::2171 0.0% 10 0.8 1.0 0.8 1.1 0.0

6.|-- fra15s29-in-x0e.1e100.net 0.0% 10 1.0 1.0 1.0 1.1 0.0

-mtr -h-help

Show all the available options.

-mtr -v-version

Show the version of the MTR command.

-mtr -r-report

This starts the report mode. In this mode, it will run the specified by “–c” number of times and show statistics at the end.

-mtr -w-report-wide

Wide report mode. The difference with the previous is that it won’t cut hostnames in the report.

17)whois

The /usr/bin/whois command searches a user name directory and displays information about the user ID or nickname specified in the Name parameter. The whois command tries to reach ARPANET host internic.net where it examines a user-name database to obtain information.

-whois .

Forces a name-only search for the name specified in the Name parameter.

-whois !

Displays help information for the nickname or handle ID specified in the Name parameter.

-whois *

Displays the entire membership list of a group or organization. If there are many members, this can take some time.

-whois ?

Requests help from the ARPANET host.

-whois -h

Specifies an alternative host name. The default host name on the ARPANET is internic.net. You can contact the other major ARPANET user-name database, nic.ddn.mil, by specifying the -h HostName flag.

18)tcpdump

tcpdump is a packet analyzer that is launched from the command line. It can be used to analyze network traffic by intercepting and displaying packets that are being created or received by the computer it's running on. It runs on Linux and most UNIX-type operating systems.

-tcpdump -I eth0

The command screen will scroll up until you interrupt and when we execute the tcpdump command it will capture from all the interfaces, however with -i switch only capture from the desired interface.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening

on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

11:33:31.976358 IP 172.16.25.126.ssh > 172.16.25.125.apwi-rxspooler: Flags [P.], seq 3500440357:3500440553, ack 3652628334, win 18760, length 196

11:33:31.976603 IP 172.16.25.125.apwi-rxspooler > 172.16.25.126.ssh: Flags [.], ack 196, win 64487, length 0

11:33:31.977243 ARP, Request who-has tecmint.com tell 172.16.25.126, length 28

11:33:31.977359 ARP, Reply tecmint.com is-at 00:14:5e:67:26:1d (oui Unknown), length 46

11:33:31.977367 IP 172.16.25.126.54807 > tecmint.com: 4240+ PTR? 125.25.16.172.inaddr.arpa. (44)

11:33:31.977599 IP tecmint.com > 172.16.25.126.54807: 4240 NXDomain 0/1/0 (121)

11:33:31.977742 IP 172.16.25.126.44519 > tecmint.com: 40988+ PTR? 126.25.16.172.inaddr.arpa. (44)

11:33:32.028747 IP 172.16.20.33.netbios-ns > 172.16.31.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST

11:33:32.112045 IP 172.16.21.153.netbios-ns > 172.16.31.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST

11:33:32.115606 IP 172.16.21.144.netbios-ns > 172.16.31.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST

11:33:32.156576 ARP, Request who-has 172.16.16.37 tell old-oraclehp1.midcorp.midday.com, length 46

11:33:32.348738 IP tecmint.com > 172.16.25.126.44519: 40988 NXDomain 0/1/0 (121)

-tcp -c 5 -I eth0

When you run the tcpdump command it will capture all the packets for the specified interface, until you hit the cancel button. But using -c option, you can capture a specified number of packets. The below example will only capture 6 packets.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening

on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

11:40:20.281355 IP 172.16.25.126.ssh > 172.16.25.125.apwi-rxspooler: Flags [P.], seq 3500447285:3500447481, ack 3652629474, win 18760, length 196

11:40:20.281586 IP 172.16.25.125.apwi-rxspooler > 172.16.25.126.ssh: Flags [.], ack 196, win 65235, length 0

11:40:20.282244 ARP, Request who-has tecmint.com tell 172.16.25.126, length 28

11:40:20.282360 ARP, Reply tecmint.com is-at 00:14:5e:67:26:1d (oui Unknown), length 46

11:40:20.282369 IP 172.16.25.126.53216 > tecmint.com.domain: 49504+ PTR? 125.25.16.172.in-addr.arpa. (44)

11:40:20.332494 IP tecmint.com.netbios-ssn > 172.16.26.17.nimaux: Flags [P.], seq 3058424861:3058424914, ack 693912021, win 64190, length 53 NBT Session Packet: Session Message

6 packets captured

23 packets received by filter

0 packets dropped by kernel

-tcpdump -A -I eth0

The below tcpdump command with the option -A displays the package in ASCII format. It is a character-encoding scheme format.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening

on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

09:31:31.347508 IP 192.168.0.2.ssh > 192.168.0.1.nokia-ann-ch1: Flags [P.], seq 3329372346:3329372542, ack 4193416789, win 17688, length 196

M.r0...vUP.E.X.....~.%..>N..oFk.....KQ..)Eq.d.,....r^l.....m\.oyE....-....g~m..Xy.6..1.....c.O.@...o_..J....i.*.....2f.mQH...Q.c...6....9.v.gb.....;..4.).UiCY]..9..x.)..Z.XF....'|..E.....M..u.5.....ul

09:31:31.347760 IP 192.168.0.1.nokia-ann-ch1 > 192.168.0.2.ssh: Flags [.], ack 196, win 64351, length 0

M....vU.r1~P.._.....

^C09:31:31.349560 IP 192.168.0.2.46393 > b.resolvers.Level3.net.domain: 11148+ PTR? 1.0.168.192.in-addr.arpa. (42)

E..F..@.@.....9.5.2.f+.....1.0.168.192.in-addr.arpa.....

3 packets captured

11 packets received by filter

0 packets dropped by kernel

-tcpdump -D

To list the number of available interfaces on the system, run the following command with -D option. 1.eth0

2.eth1

3.usbmon1 (USB bus number 1)

4.usbmon2 (USB bus number 2)

5.usbmon3 (USB bus number 3)

6.usbmon4 (USB bus number 4)

7.usbmon5 (USB bus number 5)

8.any (Pseudo-device that captures on all interfaces)

9.lo

-tcpdump -XX -I eth0

The following command with option -XX capture the data of each packet, including its link level header in HEX and ASCII format.

tcpdump -i eth0

11:51:18.974360 IP 172.16.25.126.ssh > 172.16.25.125.apwi-rxspooler: Flags [P.], seq 3509235537:3509235733, ack 3652638190, win 18760, length 196 0x0000: b8ac 6f2e 57b3 0001 6c99 1468 0800 4510 ..o.W...l..h..E.

0x0010: 00ec 8783 4000 4006 275d ac10 197e ac10 ....@.@.']...~..

0x0020: 197d 0016 1129 d12a af51 d9b6 d5ee 5018 .}...).*.Q....P. 0x0030: 4948 8bfa 0000 0e12 ea4d 22d1 67c0 f123 IH.....M".g..# 0x0040: 9013 8f68 aa70 29f3 2efc c512 5660 4fe8 ...h.p).....V`O.

0x0050: 590a d631 f939 dd06 e36a 69ed cac2 95b6 Y..1.9...ji.....

0x0060: f8ba b42a 344b 8e56 a5c4 b3a2 ed82 c3a1 ...*4K.V.....

0x0070: 80c8 7980 11ac 9bd7 5b01 18d5 8180 4536 ..y.....[.....E6

0x0080: 30fd 4f6d 4190 f66f 2e24 e877 ed23 8eb0 0.OmA..o.$.w.#..

0x0090: 5a1d f3ec 4be4 e0fb 8553 7c85 17d9 866f Z...K....S|....o

0x00a0: c279 0d9c 8f9d 445b 7b01 81eb 1b63 7f12 .y....D[{....c..

0x00b0: 71b3 1357 52c7 cf00 95c6 c9f6 63b1 ca51 q..WR.....c..Q

0x00c0: 0ac6 456e 0620 38e6 10cb 6139 fb2a a756 ..En..8...a9.*.V

0x00d0: 37d6 c5f3 f5f3 d8e8 3316 d14f d7ab fd93 7.....3..O....

0x00e0: 1137 61c1 6a5c b4d1 ddda 380a f782 d983 .7a.j\....8.....

0x00f0: 62ff a5a9 bb39 4f80 668a b....9O.f.

11:51:18.974759 IP 172.16.25.126.60952 > mddc-01.midcorp.mid-day.com.domain: 14620+ PTR? 125.25.16.172.in-addr.arpa. (44)

0x0000: 0014 5e67 261d 0001 6c99 1468 0800 4500 ..^g&...l..h..E.

0x0010: 0048 5a83 4000 4011 5e25 ac10 197e ac10 .HZ.@.@.^%...~..

0x0020: 105e ee18 0035 0034 8242 391c 0100 0001 .^...5.4.B9.....

0x0030: 0000 0000 0000 0331 3235 0232 3502 3136 ....125.25.16

0x0040: 0331 3732 0769 6e2d 6164 6472 0461 7270 .172.in-addr.arp

0x0050: 6100 000c 0001