

CS F303 Computer Networks Lab-2

Q. Find network commands to do the following.

1. See the statistics of TCP and UDP ports on Linux machine

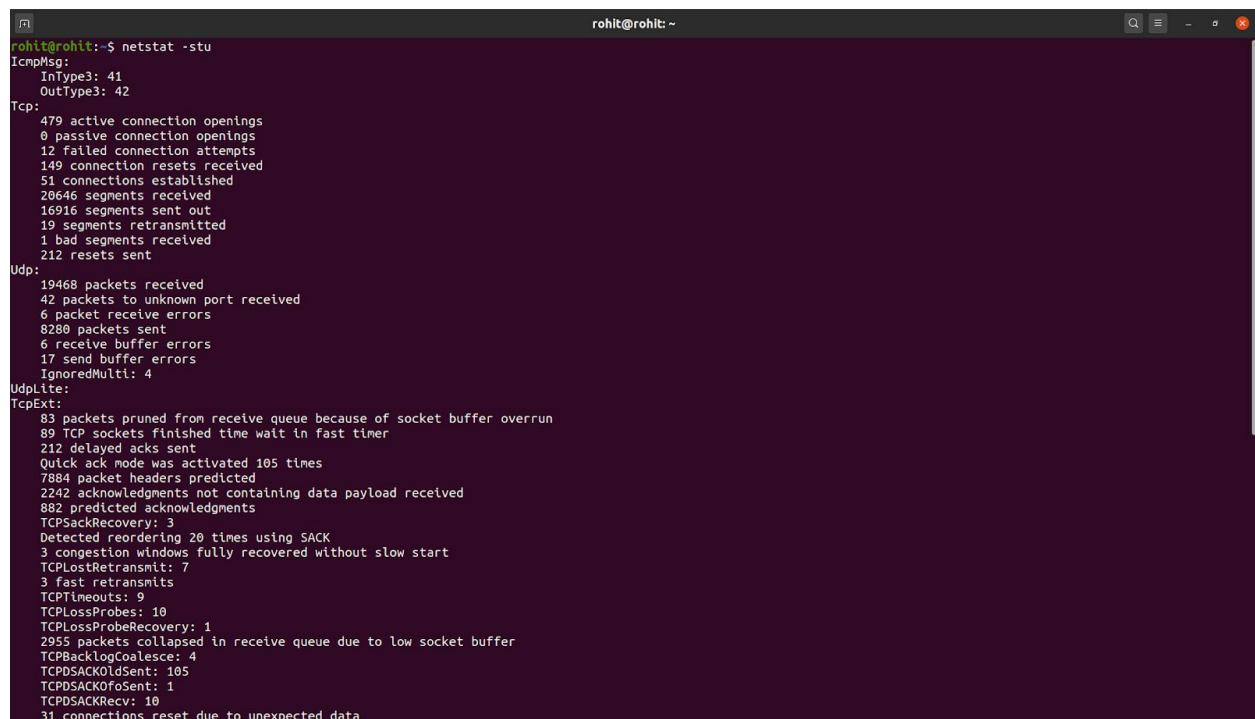
Method-1

'netstat -stu' lists the statistics including connection requests, packets sent, segments information for TCP and UDP ports on the machine.

'-s' attribute lists the statistics of each protocol.

'-t' attribute lists TCP ports.

'-u' attribute lists UDP ports.

A terminal window with a dark purple background and white text. The title bar shows 'rohit@rohit: ~'. The command 'netstat -stu' has been executed. The output is as follows:

```
rohit@rohit:~$ netstat -stu
IcmpMsg:
  InType3: 41
  OutType3: 42
Tcp:
  479 active connection openings
  0 passive connection openings
  12 failed connection attempts
  149 connection resets received
  51 connections established
  28646 segments received
  16916 segments sent out
  19 segments retransmitted
  1 bad segments received
  212 resets sent
Udp:
  19468 packets received
  42 packets to unknown port received
  6 packet receive errors
  8280 packets sent
  6 receive buffer errors
  17 send buffer errors
  IgnoredMulti: 4
UdpLite:
TcpExt:
  83 packets pruned from receive queue because of socket buffer overrun
  89 TCP sockets finished time wait in fast timer
  212 delayed acks sent
  Quick ack mode was activated 105 times
  7884 packet headers predicted
  2242 acknowledgments not containing data payload received
  882 predicted acknowledgments
  TCPSackRecovery: 3
  Detected reordering 20 times using SACK
  3 congestion windows fully recovered without slow start
  TCPLostRetransmit: 7
  3 fast retransmits
  TCPTimeouts: 9
  TCPLossProbes: 10
  TCPLossProbeRecovery: 1
  2955 packets collapsed in receive queue due to low socket buffer
  TCPBacklogCoalesce: 4
  TCPSACKOldSent: 105
  TCPSACKOldSent: 1
  TCPSACKRecv: 10
  31 connections reset due to unexpected data
```

```
rohit@rohit: ~  
TCPsackRecovery: 3  
Detected reordering 20 times using SACK  
3 congestion windows fully recovered without slow start  
TCPlostRetransmit: 7  
3 fast retransmits  
TCPTimeouts: 9  
TCPlossProbes: 10  
TCPlossProbeRecovery: 1  
2955 packets collapsed in receive queue due to low socket buffer  
TCPBacklogCoalesce: 4  
TCPDSACKOldSent: 105  
TCPDSACKOfoSent: 1  
TCPDSACKRecv: 10  
31 connections reset due to unexpected data  
97 connections reset due to early user close  
2 connections aborted due to timeout  
TCPsackShifted: 1  
TCPsackShiftFallback: 29  
TCPRecvCoalesce: 8125  
TCPFOQueue: 3343  
TCPFOMerge: 1  
TCPChallengeACK: 1  
TCPSYNChallenge: 1  
TCPAutoCorking: 121  
TCPFromZeroWindowAdv: 2  
TCPToZeroWindowAdv: 2  
TCPWantZeroWindowAdv: 90  
TCPOrigDataSent: 3425  
TCPACKSkippedSeq: 1  
TCPKeepAlive: 905  
TCPDelivered: 3831  
TCPAckCompressed: 2365  
IpExt:  
InMcastPkts: 122  
OutMcastPkts: 86  
InBcastPkts: 4  
OutBcastPkts: 4  
InOctets: 71708007  
OutOctets: 5791102  
InMcastOctets: 15618  
OutMcastOctets: 10641  
InBcastOctets: 310  
OutBcastOctets: 310  
InNoECTPkts: 61852  
rohit@rohit:~$
```

2. Enlist the listening ports on your machine

Method-1: netstat -l lists out all ports that are being listened on (STATE = LISTEN)

- -l - Show only listening ports.

NOTE: grep command can also be used additionally to highlight the listening ones but the above command will suffice our need.

Method-2: sudo ss -tunlp works in a similar fashion to above command. It lists out all listening TCP or UDP ports, including the services using the ports and the socket status along with their process IDs or PIDs.

```
rohit@rohit:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp            0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp      [::]:*                  LISTEN
udp        0      0 0.0.0.0:42971          0.0.0.0:*               *
udp        0      0 localhost:domain        0.0.0.0:*               *
udp        0      0 0.0.0.0:631            0.0.0.0:*               *
udp        0      0 224.0.0.251:mdns       0.0.0.0:*               *
udp        0      0 224.0.0.251:mdns       0.0.0.0:*               *
udp        0      0 0.0.0.0:mdns           0.0.0.0:*               *
udp6       0      0 [::]:41657             [::]:*                  *
udp6       0      0 [::]:mdns               [::]:*                  *
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7

Active UNIX domain sockets (only servers)
Proto RefCnt Flags   Type       State       I-Node   Path
unix   2      [ ACC ] STREAM    LISTENING   42848    @/tmp/dbus-Q7T4JNyc
unix   2      [ ACC ] SEQPACKET LISTENING   20901    /run/udev/control
unix   2      [ ACC ] STREAM    LISTENING   56460    /run/user/1000/systemd/private
unix   2      [ ACC ] STREAM    LISTENING   56465    /run/user/1000/bus
unix   2      [ ACC ] STREAM    LISTENING   56466    /run/user/1000/gnupg/S.dirmngr
unix   2      [ ACC ] STREAM    LISTENING   56467    /run/user/1000/gnupg/S.gpg-agent.browser
unix   2      [ ACC ] STREAM    LISTENING   56468    /run/user/1000/gnupg/S.gpg-agent.extra
unix   2      [ ACC ] STREAM    LISTENING   56469    /run/user/1000/gnupg/S.gpg-agent.ssh
unix   2      [ ACC ] STREAM    LISTENING   56470    /run/user/1000/gnupg/S.gpg-agent
unix   2      [ ACC ] STREAM    LISTENING   56471    /run/user/1000/pk-debconf-socket
unix   2      [ ACC ] STREAM    LISTENING   56472    /run/user/1000/pulse/native
unix   2      [ ACC ] STREAM    LISTENING   56473    /run/user/1000/snapd-session-agent.socket
unix   2      [ ACC ] STREAM    LISTENING   42112    /run/acpid.socket
unix   2      [ ACC ] STREAM    LISTENING   58740    @/tmp/.ICE-unix/2523
unix   2      [ ACC ] STREAM    LISTENING   54419    @/tmp/.X11-unix/X0
unix   2      [ ACC ] STREAM    LISTENING   53453    /run/user/1000/keyring/control
unix   2      [ ACC ] STREAM    LISTENING   56534    @/tmp/dbus-jlG5dJtf
unix   2      [ ACC ] STREAM    LISTENING   54088    /run/user/1000/keyring/pkcs11
unix   2      [ ACC ] STREAM    LISTENING   58768    /run/user/1000/keyring/ssh
unix   2      [ ACC ] STREAM    LISTENING   42114    /run/avahi-daemon/socket
unix   2      [ ACC ] STREAM    LISTENING   42116    /run/cups/cups.sock
unix   2      [ ACC ] STREAM    LISTENING   42118    /run/dbus/system_bus_socket
unix   2      [ ACC ] STREAM    LISTENING   42120    /run/snapd.socket
unix   2      [ ACC ] STREAM    LISTENING   42122    /run/snapd-snap.socket
unix   2      [ ACC ] STREAM    LISTENING   42124    /run/utidd/request
unix   2      [ ACC ] STREAM    LISTENING   54420    /tmp/.X11-unix/X0
unix   2      [ ACC ] STREAM    LISTENING   20874    /run/striscmd/private
```

```
rohit@rohit:~$ netstat -l
Active UNIX domain sockets (only servers)
Proto RefCnt Flags   Type       State       I-Node   Path
unix   2      [ ACC ] STREAM    LISTENING   42848    @/tmp/dbus-Q7T4JNyc
unix   2      [ ACC ] SEQPACKET LISTENING   20901    /run/udev/control
unix   2      [ ACC ] STREAM    LISTENING   56460    /run/user/1000/systemd/private
unix   2      [ ACC ] STREAM    LISTENING   56465    /run/user/1000/bus
unix   2      [ ACC ] STREAM    LISTENING   56466    /run/user/1000/gnupg/S.dirmngr
unix   2      [ ACC ] STREAM    LISTENING   56467    /run/user/1000/gnupg/S.gpg-agent.browser
unix   2      [ ACC ] STREAM    LISTENING   56468    /run/user/1000/gnupg/S.gpg-agent.extra
unix   2      [ ACC ] STREAM    LISTENING   56469    /run/user/1000/gnupg/S.gpg-agent.ssh
unix   2      [ ACC ] STREAM    LISTENING   56470    /run/user/1000/gnupg/S.gpg-agent
unix   2      [ ACC ] STREAM    LISTENING   56471    /run/user/1000/pk-debconf-socket
unix   2      [ ACC ] STREAM    LISTENING   56472    /run/user/1000/pulse/native
unix   2      [ ACC ] STREAM    LISTENING   56473    /run/user/1000/snapd-session-agent.socket
unix   2      [ ACC ] STREAM    LISTENING   42112    /run/acpid.socket
unix   2      [ ACC ] STREAM    LISTENING   58740    @/tmp/.ICE-unix/2523
unix   2      [ ACC ] STREAM    LISTENING   54419    @/tmp/.X11-unix/X0
unix   2      [ ACC ] STREAM    LISTENING   53453    /run/user/1000/keyring/control
unix   2      [ ACC ] STREAM    LISTENING   56534    @/tmp/dbus-jlG5dJtf
unix   2      [ ACC ] STREAM    LISTENING   54088    /run/user/1000/keyring/pkcs11
unix   2      [ ACC ] STREAM    LISTENING   58768    /run/user/1000/keyring/ssh
unix   2      [ ACC ] STREAM    LISTENING   42114    /run/avahi-daemon/socket
unix   2      [ ACC ] STREAM    LISTENING   42116    /run/cups/cups.sock
unix   2      [ ACC ] STREAM    LISTENING   42118    /run/dbus/system_bus_socket
unix   2      [ ACC ] STREAM    LISTENING   42120    /run/snapd.socket
unix   2      [ ACC ] STREAM    LISTENING   42122    /run/snapd-snap.socket
unix   2      [ ACC ] STREAM    LISTENING   42124    /run/utidd/request
unix   2      [ ACC ] STREAM    LISTENING   54420    /tmp/.X11-unix/X0
unix   2      [ ACC ] STREAM    LISTENING   20874    /run/striscmd/private
unix   2      [ ACC ] STREAM    LISTENING   57642    /tmp/ssh-ubU2NLX0dIn6/agent.2354
unix   2      [ ACC ] STREAM    LISTENING   20876    /run/systemd/userdb/io.systemd.DynamicUser
unix   2      [ ACC ] STREAM    LISTENING   58741    /tmp/.ICE-unix/2523
unix   2      [ ACC ] STREAM    LISTENING   40416    /run/irqbalance/irqbalance1311.sock
unix   2      [ ACC ] STREAM    LISTENING   20887    /run/systemd/fscck.progress
unix   2      [ ACC ] STREAM    LISTENING   42847    @/tmp/dbus-PNSaCmhm
unix   2      [ ACC ] STREAM    LISTENING   20897    /run/systemd/journal/stdout
unix   2      [ ACC ] STREAM    LISTENING   16673    /run/systemd/journal/io.systemd.journal
unix   2      [ ACC ] STREAM    LISTENING   56533    @/tmp/dbus-RVF0nPET
unix   2      [ ACC ] STREAM    LISTENING   54602    @/home/rohit/.cache/ibus/dbus-xFiyCcJp
unix   2      [ ACC ] STREAM    LISTENING   60968    /tmp/.org.chromium.Chromium.Ba6Nra/SingletonSocket
unix   2      [ ACC ] STREAM    LISTENING   47651    /var/run/mysqld/mysqld.sock
unix   2      [ ACC ] STREAM    LISTENING   45726    /var/snap/canonical-livepatch/95/livepatchd-priv.sock
unix   2      [ ACC ] STREAM    LISTENING   45727    /var/snap/canonical-livepatch/95/livepatchd.sock
unix   2      [ ACC ] STREAM    LISTENING   53979    @/tmp/dbus-l5nCM7qHR
```

```

rohit@rohit:~$ sudo ss -tunlp
[sudo] password for rohit:
Netid      State      Recv-Q     Send-Q      Local Address:Port      Peer Address:Port      Process
udp        UNCONN    0           0           0.0.0.0:42971          0.0.0.0:*               users:({"avahi-daemon",pid=1283,fd=14})
udp        UNCONN    0           0           127.0.0.53%lo:53       0.0.0.0:*               users:({"systemd-resolve",pid=1251,fd=12})
udp        UNCONN    0           0           0.0.0.0:631           0.0.0.0:*               users:({"cups-browsed",pid=1427,fd=7})
udp        UNCONN    0           0           224.0.0.251:5353       0.0.0.0:*               users:({"chrome",pid=2933,fd=175})
udp        UNCONN    0           0           224.0.0.251:5353       0.0.0.0:*               users:({"chrome",pid=2933,fd=170})
udp        UNCONN    0           0           0.0.0.0:5353          0.0.0.0:*               users:({"avahi-daemon",pid=1283,fd=12})
udp        UNCONN    0           0           [::]:41657            [::]:*                  users:({"avahi-daemon",pid=1283,fd=15})
udp        UNCONN    0           0           [::]:5353             [::]:*                  users:({"avahi-daemon",pid=1283,fd=13})
tcp        LISTEN    0           80           127.0.0.1:3306         0.0.0.0:*               users:({"mysqld",pid=1543,fd=17})
tcp        LISTEN    0           4096          127.0.0.53%lo:53       0.0.0.0:*               users:({"systemd-resolve",pid=1251,fd=13})
tcp        LISTEN    0           5            127.0.0.1:631         0.0.0.0:*               users:({"cupsd",pid=1286,fd=7})
tcp        LISTEN    0           5            [::]:631              [::]:*                  users:({"cupsd",pid=1286,fd=6})
rohit@rohit:~$

```

3. See the mail xchange (MX) record for www.gmail.com

Method-1

nslookup -type=MX www.gmail.com

'nslookup' command opens up an interactive session where one needs to 'set type = MX' followed by the domain name www.gmail.com and values Corresponding to mail exchanger are the MX values.

Method-2

'dig -t MX gmail.com' command list out MX records in the Answer Section.

```
rohit@rohit:~$ dig -t mx www.gmail.com
;<<> DiG 9.16.1-Ubuntu <<> -t mx www.gmail.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 64830
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.gmail.com.                IN      MX
;; ANSWER SECTION:
www.gmail.com.                600     IN      CNAME   mail.google.com.
mail.google.com.              599     IN      CNAME   googlemail.l.google.com.
;; Query time: 88 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Feb 01 18:35:00 IST 2021
;; MSG SIZE rcvd: 95

rohit@rohit:~$ nslookup -q=MX gmail.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
gmail.com    mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com    mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.
gmail.com    mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com    mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com    mail exchanger = 5 gmail-smtp-in.l.google.com.

Authoritative answers can be found from:

rohit@rohit:~$
```

4. Display the all network interfaces on your machine

Method-1

'ifconfig -a' command lets us view all the configurations of network interfaces including those that are currently inactive.

Method-2

'Netstat -i' command shows the state of the all network interfaces that are configured on the local system.

```
rohit@rohit:~$ ifconfig -a
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2875 bytes 307590 (307.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2875 bytes 307590 (307.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.21 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::f2ca:3b93:f7cc:8e39 prefixlen 64 scopeid 0x20<link>
    ether 28:c6:3f:9e:57:d2 txqueuelen 1000 (Ethernet)
    RX packets 111280 bytes 114167845 (114.1 MB)
    RX errors 0 dropped 2521 overruns 0 frame 0
    TX packets 56497 bytes 19027968 (19.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

rohit@rohit:~$ netstat -i
Kernel Interface table
Iface MTU RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
lo 65536 2948 0 0 0 2948 0 0 0 LRU
wlo1 1500 111604 0 2620 0 56734 0 0 0 BMRU
rohit@rohit:~$
```

5. A list of intermediate routers to reach 8.8.8.8 from your machine, with latency

Method-1: sudo traceroute 8.8.8.8

traceroute command sends Internet Control Message Protocol (ICMP) packets to test connections and report on latency between two points of the Internet. The first line of the traceroute output describes what the command is doing. It lists the destination system (8.8.8.8), destination IP address (8.8.8.8), and the maximum number of hops that will be used in the traceroute (64).

The remainder of the output shows information on each hop, which is typically a router, in the path between the sender and the final destination.

```
rohit@rohit:~$ sudo traceroute 8.8.8.8
[sudo] password for rohit:
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max
 1  192.168.0.1  3.656ms  107.419ms  2.982ms
 2  10.195.128.1  11.471ms  13.221ms  12.252ms
 3  49.207.34.197  10.534ms  11.720ms  12.288ms
 4  49.207.34.161  11.953ms  11.142ms  11.612ms
 5  49.207.47.205  11.053ms  8.615ms  12.638ms
 6  10.23.206.158  11.148ms  7.795ms  11.812ms
 7  8.8.8.8  11.368ms  9.685ms  13.952ms
rohit@rohit:~$
```

6. Send 10 echo requests to 8.8.8.8 server from your machine

ping -c 10 8.8.8.8' command sends 10 echo of ICMP packages to 8.8.8.8, the number after -c specifies the number of echoes that will be sent.

```
rohit@rohit:~$ ping -c 10 www.google.com
PING www.google.com (216.58.196.100) 56(84) bytes of data:
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=1 ttl=118 time=10.1 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=2 ttl=118 time=8.04 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=3 ttl=118 time=7.70 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=4 ttl=118 time=9.30 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=5 ttl=118 time=7.67 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=6 ttl=118 time=9.50 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=7 ttl=118 time=7.47 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=8 ttl=118 time=10.4 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=9 ttl=118 time=9.90 ms
64 bytes from del11s05-in-f4.1e100.net (216.58.196.100): icmp_seq=10 ttl=118 time=10.5 ms

--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 7.474/9.057/10.482/1.149 ms
rohit@rohit:~$
```


7. Get the IP address of www.bits-pilani.ac.in domain.

Method-1:

'dig www.bits-pilani.ac.in' lists out the IP address in ANSWER Section

Method-2

'nslookup www.bits-pilani.ac.in' lists out the IP address under non-authoritative answer

```
rohit@rohit:~$ dig www.bits-pilani.ac.in
;; <<>> DiG 9.16.1-Ubuntu <<>> www.bits-pilani.ac.in
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 39477
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.bits-pilani.ac.in.      IN      A
;; ANSWER SECTION:
www.bits-pilani.ac.in.  600     IN      CNAME   universe.bits-pilani.ac.in.
universe.bits-pilani.ac.in. 599     IN      A       103.144.92.33
universe.bits-pilani.ac.in. 599     IN      A       14.139.243.20

;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Jan 31 10:36:21 IST 2021
;; MSG SIZE rcvd: 105

rohit@rohit:~$ nslookup www.bits-pilani.ac.in
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.bits-pilani.ac.in canonical name = universe.bits-pilani.ac.in.
Name:   universe.bits-pilani.ac.in
Address: 103.144.92.33
Name:   universe.bits-pilani.ac.in
Address: 14.139.243.20

rohit@rohit:~$
```