

Computer Networks

Assignment 1

Karan Sunil Kumbhar
12140860
BTech, Cse
2025

CS301 Computer Networks



Sept 2, 2023

Basic Networking Tool

Question 1] Solution

Part 1] Answer

Here `ifconfig` stands for **interface configuration**. So `ifconfig` command in a Unix-like operating system is used for configuring and displaying network interface parameters. It enables the assignment of addresses to network interfaces and the modification of interface operating parameters. Upon system startup, the `ifconfig` command is essential for defining the network address of each interface. It is also used to alter the configuration or display the current settings of active network interfaces.

Here is the output of ifconfig in my pc :-

```
karan@karan-Inspiron-15-3511:~$ ifconfig
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 1474 bytes 152041 (152.0 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1474 bytes 152041 (152.0 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp3s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.10.17.116 netmask 255.255.252.0 broadcast 10.10.19.255
        inet6 fe80::5549:4a6c:41d5:59fc prefixlen 64 scopeid 0x20<link>
            ether 90:0f:0c:b7:be:25 txqueuelen 1000 (Ethernet)
            RX packets 54350 bytes 63556022 (63.5 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 26379 bytes 3582287 (3.5 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Important attributes that the output of `ifconfig` typically includes :-

For wlp3s0 network interface -

- **Interface Name** : This is the name of the network interface.

E.g

- `eth0, eth1` - for first and second Ethernet interfaces respectively.
- `lo` - for loopback interface(system used to communicate with itself)
- `wlan0, wlan1` - for the first and second wireless network interface on the system.

But nowadays due to complex hardware configuration desire for some descriptive names, many Linux distributions have moved to a more systematic naming convention

- `en` for Ethernet interfaces
- `wl` for wireless interfaces
- `ww` for wireless WAN interfaces
- `lo` for the loopback interface

In my case, "wlp3s0" indicates a wireless network interface with a specific PCI bus number (3) and slot number (0)

- **Flags:** UP (interface is up), BROADCAST (supports broadcast), RUNNING (interface is operational), MULTICAST (supports multicast)
- **MTU** (Maximum Transmission Unit): The maximum size of a data packet that can be transmitted over the network interface. [mtu - 1500 bytes]
- **IPv4 and IPv6 Addresses:** Displays the assigned IPv4 and IPv6 addresses, if configured.

For wlp3s0 :-

- IPv4 address inet: [10.10.17.116]
- IPv6 address inet6:[fe80::5549:4a6c:41d5:59fc]
- **MAC Address:** Also known as the hardware address, it's a unique identifier for the network interface.
 - `ether`: [90:0f:0c:b7:be:25]
- **netmask:** Subnet mask associated with the IPv4 address [255.255.252.0]
- **broadcast:** Broadcast address for the subnet [10.10.19.255]
- **prefixlen:** Length of the IPv6 prefix (64 bits)
- **scopeid:** Scope ID of the IPv6 address (`0x20<link>`)
- **ether:** MAC address of the interface (90:0f:0c:b7:be:25)
- **txqueuelen:** Transmit queue length[1000 packets]
- **RX packets 54350** - indicates that a total of 54,350 data packets have been received by the network interface.
- **TX packets 26379** - indicates that a total of 26,379 data packets have been transmitted by the network interface.
- **RX errors 0** and **TX errors 0** indicate that no errors have been reported during the reception or transmission of packets, respectively.

Part 2] Answer

The `ifconfig` command offers several options to configure and manipulate network interfaces. Here are explanations for four important options:

1. `-a` (Display All Interfaces):

- When used without an interface name, this option displays the status of all currently available network interfaces, both active and inactive.

- Useful for getting a comprehensive overview of all interfaces, including loopback and physical ones.

2. **-s (Short Display):**

- This option provides a short and summarized list of network interfaces, similar to the output of the `netstat -i` command.
- It's handy for quickly viewing the names of interfaces without detailed information.

3. **up:**

- When you specify the `up` flag, it activates the network interface.
- This flag is implicitly set when an IP address is assigned to the interface.
- It is used to bring the interface into an operational state, allowing it to send and receive network traffic.

4. **down:**

- When you specify the `down` flag, it deactivates or shuts down the network interface.
- This flag causes the driver for the interface to be disabled, effectively disabling network communication on that interface.
- Useful when you want to temporarily stop network traffic on an interface, such as for maintenance or troubleshooting.

Examples :-

1.

```
karan@karan-Inspiron-15-3511:~$ 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 64252 bytes 10435881 (10.4 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 64252 bytes 10435881 (10.4 MB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

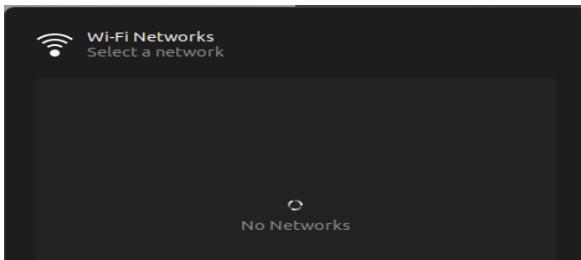
wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.10.76.149 netmask 255.255.240.0 broadcast 10.10.79.255
      inet6 fe80::5549:4a6c:41d5:59fc prefixlen 64 scopeid 0x20<link>
          ether 90:0f:0c:b7:be:25 txqueuelen 1000 (Ethernet)
          RX packets 7095677 bytes 9038824475 (9.0 GB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 3113466 bytes 362341480 (362.3 MB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2.

Iface	MTU	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
lo	65536	64264	0	0 0		64264	0	0	0	LRU
wlp3s0	1500	7095707	0	0 0		3113479	0	0	0	BMRU

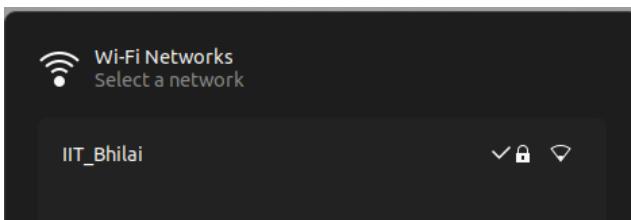
3.

```
karan@karan-Inspiron-15-3511:~$ sudo ifconfig wlp3s0 down  
[sudo] password for karan:
```



4.

```
karan@karan-Inspiron-15-3511:~$ sudo ifconfig wlp3s0 up
```



Question 2] Solution

Part 1] Answer

The `netstat` command is used to display various network-related information on a Unix-like operating system. It provides details about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Some common uses of the `netstat` command include:

- **Viewing Network Connections:** we use `netstat` to view all active network connections, both incoming and outgoing, along with their associated IP addresses, port numbers, and protocol types.
- **Displaying Routing Information:** The command can show routing tables, which list how data packets should be directed to reach their destination.

Part 2] Answer

(a) To get active TCP ports on System we can use `netstat -tn` command where each flag has different meaning

```
karan@karan-Inspiron-15-3511:~$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 10.10.76.93:49158       142.250.66.10:443    ESTABLISHED
tcp      0      0 10.10.76.93:56414       172.217.166.78:443    ESTABLISHED
tcp      0      0 10.10.76.93:53250       34.107.221.82:80     TIME_WAIT
tcp      0      0 10.10.76.93:36028       35.83.34.165:443    ESTABLISHED
tcp      0      0 10.10.76.93:45496       34.117.65.55:443    ESTABLISHED
tcp      0      0 10.10.76.93:42530       172.217.174.78:443   ESTABLISHED
tcp      0      32 10.10.76.88:58034      52.12.130.210:443   FIN_WAIT1
tcp      0      0 10.10.76.93:48116      142.250.199.170:443  ESTABLISHED
tcp      0      0 10.10.76.93:37682      34.149.100.209:443  ESTABLISHED
tcp      0      0 10.10.76.93:53246      34.107.221.82:80     TIME_WAIT
tcp      0      0 10.10.76.93:41672      142.250.192.35:443  ESTABLISHED
tcp      0      0 10.10.76.93:34020      142.250.199.161:443  ESTABLISHED
tcp      0      0 10.10.76.93:49172      142.250.66.10:443    ESTABLISHED
tcp      0      103 10.10.76.88:35474     3.230.17.121:443    FIN_WAIT1
tcp      0      0 10.10.76.93:38754      142.250.192.45:443  ESTABLISHED
tcp      0      103 10.10.76.88:45510     104.18.2.161:443    FIN_WAIT1
tcp      0      0 10.10.76.93:45498      34.117.65.55:443    ESTABLISHED
tcp      0      0 10.10.76.93:48746     35.83.34.165:443    ESTABLISHED
```

Explanation of options:

- `-t`: Show TCP ports.
- `-n`: Show numerical addresses instead of resolving hostnames.(not necessary)

(b)to identify the port and PIDs of web browser we can use `netstat -p <browser-name>`.

In my case, it is firefox

Here `-p` flag is for to mention specific program and get it's PID and name(here it is firefox) and also `--numeric-port` is to show server end port number

```
karan@karan-Inspiron-15-3511:~$ netstat -p firefox --numeric-port
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 karan-Inspiron-15:51410  82.221.107.34.bc.goo:80 ESTABLISHED 3053/firefox
tcp      0      0 10.10.74.148:38068       del11s20-in-f14.1e1:443 TIME_WAIT   -
tcp      0      0 karan-Inspiron-15:48506   hkg12s09-in-f10.1e1:443 TIME_WAIT   -
tcp      0      0 karan-Inspiron-15:49418   whatsapp-cdn-shv-01:443 ESTABLISHED 3053/firefox
tcp      0      0 karan-Inspiron-15:51394   82.221.107.34.bc.goo:80 ESTABLISHED 3053/firefox
tcp      0      0 10.10.74.148:35146       102.115.120.34.bc.g:443 TIME_WAIT   -
tcp      0      103 10.10.74.148:57362     del12s03-in-f10.1e1:443 FIN_WAIT1 -
tcp      0      0 karan-Inspiron-15:37284   bom12s11-in-f3.1e10:443 ESTABLISHED 3053/firefox
tcp      0      0 karan-Inspiron-15:49406   whatsapp-cdn-shv-01:443 ESTABLISHED 3053/firefox
tcp      0      275 10.10.74.148:57804     del12s08-in-f10.1e1:443 ESTABLISHED 3053/firefox
tcp      0      103 10.10.74.148:44166     del12s11-in-f14.1e1:443 FIN_WAIT1 -
tcp      0      0 karan-Inspiron-15:54802   bom07s36-in-f14.1e1:443 ESTABLISHED 3053/firefox
```

In output we are getting PID of web browser as **3053** and respective ports at our end are mention in Local Address column after hostname or ip address

```
tcp    0 0 karan-Inspiron-15:51410 82.221.107.34.bc.goo:80 ESTABLISHED 3053/firefox
```

Like here after hostname(karan-Inspiron-15) their is port number of specific process which is **51410** and at other end it is after Foreign address is port number at other end here it is **80**

(c) In browsers it is not easy to find specific PID and port number of specific tabs as it depends

```
karan@karan-Inspiron-15-3511:~$ netstat -ptun firefox | grep firefox
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp      0      0 10.10.76.47:46022      142.250.192.46:443      ESTABLISHED 12887/firefox
tcp      0      0 10.10.76.47:42758      34.117.65.55:443      ESTABLISHED 12887/firefox
tcp      0      0 10.10.76.47:58842      142.250.199.174:443    ESTABLISHED 12887/firefox
tcp      0      0 10.10.76.47:52252      142.251.42.42:443      ESTABLISHED 12887/firefox
tcp      0      0 10.10.76.47:58054      216.58.196.66:443      ESTABLISHED 12887/firefox
tcp      0      0 10.10.76.47:37610      34.120.208.123:443    ESTABLISHED 12887/firefox
tcp      0      0 10.10.76.47:41534      142.250.183.99:443    ESTABLISHED 12887/firefox
tcp      0      0 10.10.76.47:36272      142.251.42.67:443      ESTABLISHED 12887/firefox
```

on browser architecture and how they are processing their new processes.Identifying the specific port number and process ID (PID) of a particular tab in a web browser can be challenging, as modern web browsers often manage multiple tabs within a single process. This makes it difficult to associate a unique port number and PID with each individual tab.

As I am using firefox as a web browser we can find PID and port number all services related to firefox from the above screenshot (here PID is **12887** and port numbers are after hostname in output).But still we are not able to get port number to specific tab in browser.

We also can observe that the number of services after opening a new tab is not linearly increasing. Demonstrated as below

1. When browser is closed(no tabs were opened)

```
karan@karan-Inspiron-15-3511:~$ netstat -pntlu firefox | grep firefox | wc -l
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
0
```

2. When I opened a new tab (one tab is opened)

```
karan@karan-Inspiron-15-3511:~$ netstat -ptun firefox | grep firefox | wc -l
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
26
```

3. When I opened second tab(YouTube)

```
karan@karan-Inspiron-15-3511:~$ netstat -ptun firefox | grep firefox | wc -l
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
34
```

4. And again when I opened a third tab(Google Classroom)

```
karan@karan-Inspiron-15-3511:~$ netstat -ptun firefox | grep firefox | wc -l
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
35
```

So, by observing the above data we can say that it is not easy to find a unique port number corresponding to a specific tab.

(d)standard ports associated with HTTP, DHCP, DNS, SMTP, and FTP:

1. **HTTP (Hypertext Transfer Protocol):**

- Standard Port: 80 (TCP)
- Secure Port (HTTPS): 443 (TCP)

2. **DHCP (Dynamic Host Configuration Protocol):**

- Standard Ports:
 - DHCP Server: 67 (UDP)
 - DHCP Client: 68 (UDP)

3. **DNS (Domain Name System):**

- Standard Port: 53 (UDP and TCP)

4. SMTP (Simple Mail Transfer Protocol):

- Standard Port: 25 (TCP)

5. FTP (File Transfer Protocol):

- Standard Ports:

- FTP Control: 21 (TCP)
- FTP Data Transfer: 20 (TCP)

```
karan@karan-Inspiron-15-3511:~$ netstat -an | grep -E ":(443|80|68|67|53|25|21|20)\b"
tcp      0      0 127.0.0.53:53          0.0.0.0:*                  LISTEN
tcp      0      0 10.10.19.76:47840     216.58.203.10:443      ESTABLISHED
tcp      0      0 10.10.19.76:47830     216.58.203.10:443      ESTABLISHED
tcp      0      0 10.10.19.76:38146     74.125.169.71:443      ESTABLISHED
tcp      0      0 10.10.19.76:36340     142.251.42.46:443      ESTABLISHED
tcp      0      32 10.10.19.107:44406    54.218.18.184:443      FIN_WAIT1
tcp      0      0 10.10.19.76:53842     34.117.65.55:443      ESTABLISHED
tcp      0      0 10.10.19.76:52868     142.250.192.110:443      ESTABLISHED
tcp      0      103 10.10.19.107:53834   142.250.199.142:443      FIN_WAIT1
tcp      0      0 10.10.19.76:41608     35.83.34.165:443      ESTABLISHED
tcp      0      0 10.10.19.76:52822     172.217.160.206:443      ESTABLISHED
tcp      0      0 10.10.19.76:54406     142.250.183.131:443      TIME_WAIT
tcp      0      0 10.10.19.76:46994     142.250.199.142:443      ESTABLISHED
udp      0      0 127.0.0.53:53          0.0.0.0:*                  LISTEN
udp      0      0 10.10.19.76:68          10.200.10.250:67        ESTABLISHED
```

So, on my computer only DNS standard port(53) and DHCP client port(68) is used to run the service

Part 3] Answer

To show the statistics of all UDP connections using the `netstat` command, we can use the `-su` option. This option displays a summary of UDP protocol statistics. Here's how we can use it:

```
karan@karan-Inspiron-15-3511:~$ netstat -su
IcmpMsg:
    InType0: 7
    InType3: 714
    InType8: 36
    InType11: 100
    OutType0: 36
    OutType3: 752
    OutType8: 14
Udp:
    189914 packets received
    412 packets to unknown port received
    0 packet receive errors
    130805 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 3
UdpLite:
IpExt:
    InMcastPkts: 482
    OutMcastPkts: 551
    InBcastPkts: 3
    OutBcastPkts: 3
    InOctets: 5405686197
    OutOctets: 148166276
    InMcastOctets: 69846
    OutMcastOctets: 74846
    InBcastOctets: 234
    OutBcastOctets: 234
    InNoECTPkts: 4404202
    InECT0Pkts: 19
MPTcpExt:
```

Question 3] Solution

Part 1] Answer

The `ping` command is a network utility tool used to test the reachability and latency of a remote host or server over a network, most commonly using the Internet Control Message Protocol (ICMP). It's a basic and widely used tool for diagnosing network connectivity issues, measuring response times, and checking the general health of a network connection. Here are the main uses of the `ping` command:

1. **Checking Network Reachability:** The primary purpose of the `ping` command is to determine if a remote host or IP address is reachable over the network. By sending ICMP Echo Request packets to the target host, the command waits for ICMP Echo Reply packets to confirm if the target is online and responding.
2. **Measuring Round-Trip Time (RTT):** `ping` also provides information about the round-trip time (RTT) it takes for a packet to travel from the source to the destination and back. The reported RTT helps in understanding the latency or delay in the network connection.

Part 2] Answer

(a)IP addresses of some famous and commonly used hosts:

1. **Harvard University [US]**
 - Website: www.harvard.edu
 - IP Address: 151.101.42.133
 2. **Shanghai Jiao Tong University [China]**
 - Website: www.sjtu.edu.cn
 - IP Address: 202.120.2.119
 3. **Indian Institute of Science (IISc) [India]**
 - Website: www.iisc.ac.in
 - IP Address: 20.192.9.200
-
- Calculating RTT
 - 1. Harvard University [151.101.42.133]

Sr. No.	Morning [3:00 AM]	Evening [6:00 PM]	Night [9:00 PM]
1	86.232	21.562	1079.537
2	113.371	43.904	1628.238
3	88.951	44.212	337.116
4	85.551	22.087	311.177
5	84.56	20.232	377.603
6	129.815	22.942	282.119
7	85.238	29.329	724.469
8	90.866	51.911	231.858
9	85.36	94.323	76.4
10	121.013	43.024	242.241
Average	97.0957	39.3526	529.0758

2. Shanghai Jiao Tong University [202.120.2.119]

Sr. No.	Morning [3:00 AM]	Evening [6:00 PM]	Night [9:00 AM]
1	439.714	457.271	524.698
2	460.663	454.583	656.146
3	493.969	490.775	826.815
4	835.701	457.684	1313.446
5	497.648	521.763	902.149
6	439.506	527.085	665.895
7	439.616	456.548	659.42
8	490.216	455.991	525.003
9	440.412	455.685	633.375
10	439.828	496.319	696.909
Average	497.7273	477.3704	740.3856

3. Indian Institute of Science (IISc) [20.192.9.200]

Sr. No.	Morning [3:00 AM]	Evening [6:00 PM]	Night [9:00 AM]
1	23.768	64.768	433.222
2	25.937	45.996	1837.36
3	38.738	136.863	3214.807
4	42.749	22.498	557.063
5	29.339	21.462	167.373
6	24.316	33.918	180.79
7	68.909	77.328	666.319
8	27.866	46.12	1154.995
9	35.762	36.911	378.084
10	27.139	30.537	226.76
Average	34.4523	51.6401	881.6773

Here it is not easy to get correlation between geolocation and RTT as IISC shows less time than Harvard University but also shows less time than IISC on another hour.

RTT can be influenced by various factors, including network congestion, routing, and server load. While there might be some correlation between RTT and geographical distance, it's not always a direct relationship due to the complexity of the internet's infrastructure. In summary, while there can be a correlation between RTT and geographical distance, it's not the only factor at play.(but it is typically increases with distance)

(b)Varying Package Size

Host :- Harvard University(www.harvard.edu)

As here we can see RTT increases as packet size increase in most places but not always correct as sometimes it is also decreasing. Also some hour of day for same size package it is also not same possibly due to network traffic not same on each of the mentioned time

The impact of packet size and time of day on RTT can be complex. Larger packet sizes can lead to increased transmission times and potentially higher RTT. Time of day can influence network congestion, which can in turn affect RTT. Network congestion tends to be higher during peak hours.

Packet Size (Bytes)	Morning RTT [3:00 AM]	Evening RTT [6:00 PM]	Night RTT [9:00 AM]
144	19.841	126.754	123.528
224	58.322	19.725	51.901
304	48.281	19.331	35.959
384	63.391	19.322	211.596
464	62.543	57.889	31.046
544	44.392	35.065	28.331
624	19.828	43.461	50.235
704	19.42	19.51	62.31
784	41.212	42.541	88.26
864	38.672	39.496	190.134

In summary, both packet size and time of day can impact RTT. Larger packet sizes might lead to higher RTT due to longer transmission times, and time of day can influence network congestion and overall network performance. It's important to note that various factors can contribute to RTT variations, and the relationship may not be linear. (**Graphs are in images directory under Part1_Q3_q2_b_subdirectory**)

Question 4] Solution

Part 1] Answer

A traceroute gives us a map or path for how data travels through the internet from source to the destination. More formally we can say, the traceroute tool is used to trace the route that data packets take from a source to a destination over a network, such as the Internet. It helps identify the path that data follows, the number of hops (intermediate network devices), and the time it takes for packets to travel to each hop. Traceroute is particularly useful for:

- 1. Network Troubleshooting:** Traceroute helps identify network issues, such as slow connections, packet loss, or routing problems. By showing the path and the time taken to reach each hop.
- 2. Determining Network Path:** Traceroute provides insight into the network path that data packets take to reach their destination. This can be useful for understanding how data is routed through different networks and ISPs.

In essence, traceroute provides valuable insights into the path and performance of data packets as they travel across networks, aiding in diagnosing and resolving network-related problems.

Part 2] Answer

Traceroute may not always find complete paths to some hosts due to various reasons, including network configurations, security measures, and the behavior of certain routers. Here are some common scenarios where traceroute might not show complete paths:

- 1. Firewalls and Filtering:** Some hosts or routers may have firewalls or filtering rules that prevent them from responding to traceroute requests. This is often done for security reasons to avoid exposing network information to potential attackers. As a result, traceroute may show timeouts for these hosts.
- 2. ICMP Filtering:** Traceroute primarily relies on ICMP (Internet Control Message Protocol) packets to gather information about the route. If ICMP packets are filtered or blocked by some routers along the path, traceroute might not receive the necessary responses to map the complete path.
- 3. Load Balancing:** Some networks employ load balancing techniques that distribute traffic across multiple routes. This can cause packets from a single traceroute to take different paths, leading to incomplete or inconsistent results.
- 4. Rate Limiting:** To prevent abuse or excessive traffic, routers may implement rate limiting on ICMP responses. This can result in incomplete paths as some routers might not respond to all traceroute requests.

In summary, traceroute may not always find complete paths due to network policies, security measures, filtering, and the dynamic nature of internet routing. When encountering

incomplete paths, it's essential to consider these factors and remember that traceroute results can vary based on network conditions and configurations.

Part 3] Answer

Yes, it is possible to attempt to find the route to certain hosts that fail to respond with the ping experiment using the `traceroute` tool. While the `ping` utility sends ICMP echo request packets to the destination host and expects an ICMP echo reply in response, `traceroute` uses a different approach to trace the route taken by packets to the destination.

Here's why `traceroute` might be able to provide information even when `ping` fails:

1. **ICMP Filtering:** Some hosts or routers may filter or block ICMP packets, including ping requests, as a security measure. However, they might still allow other types of ICMP messages, such as the "Time Exceeded" message, which is used by `traceroute` to identify hops along the route. Therefore, even if a host doesn't respond to ICMP echo requests (ping), it might still respond to other ICMP messages used by `traceroute`.
2. **Unresponsive Hosts vs. Routers:** Hosts might be unresponsive to ping requests, but routers along the route might still generate the necessary ICMP "Time Exceeded" messages. These messages are essential for `traceroute` to determine the route and measure the time taken to reach each hop.

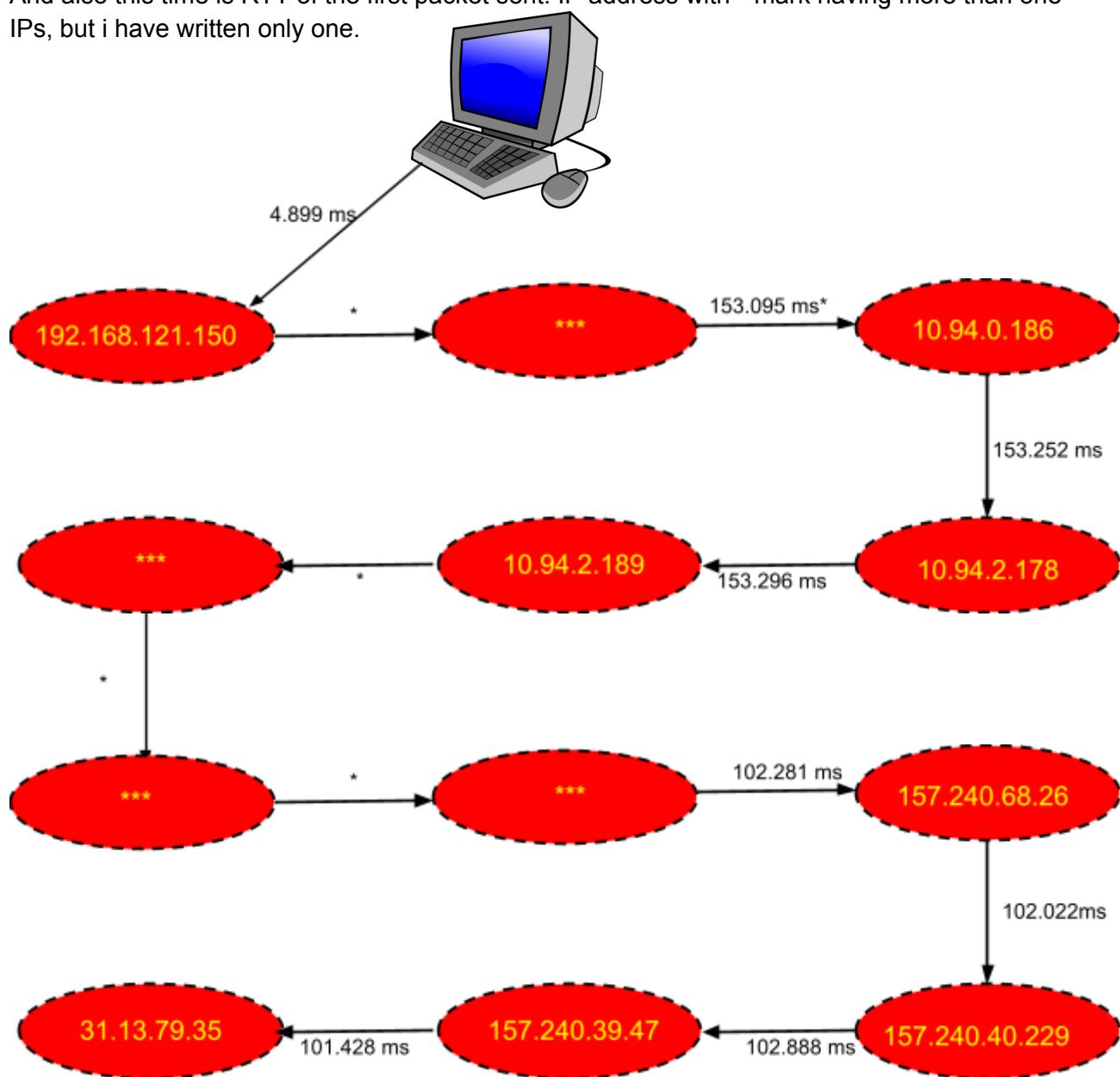
While `traceroute` can often provide route information even when `ping` requests fail, it's important to note that the results might not always be complete or accurate due to various network factors and configurations. Additionally, some hosts might be configured to not respond to any kind of probe, in which case both `ping` and `traceroute` could yield limited results.

Part 4] Answer

(Complete graph is in images folder in Part1_Q4_q4)

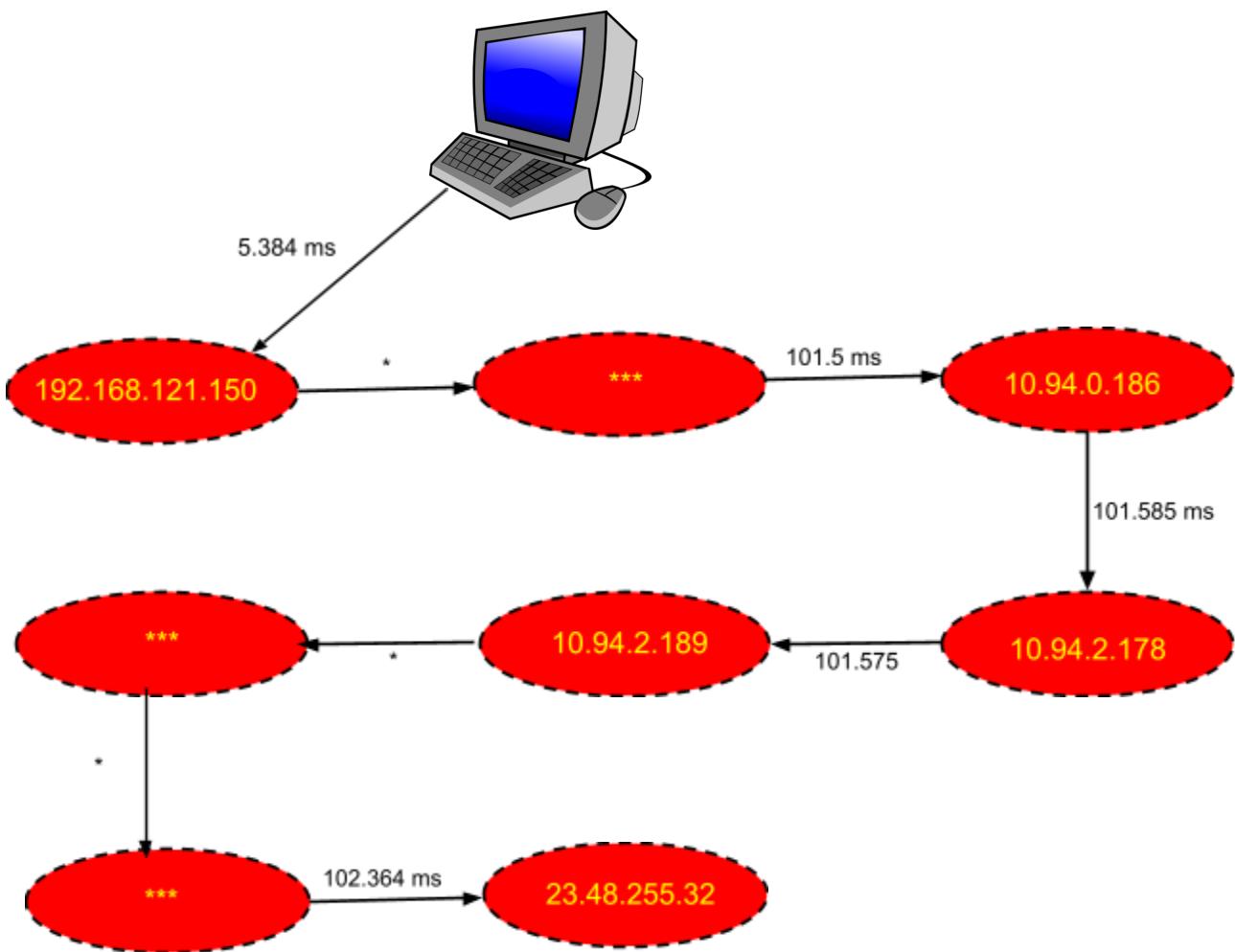
1] www.facebook.com

Here I am mentioning the RTT of the router at the [x] node on the link joining [x-1] and [x] node. And also this time is RTT of the first packet sent. IP address with * mark having more than one IPs, but i have written only one.



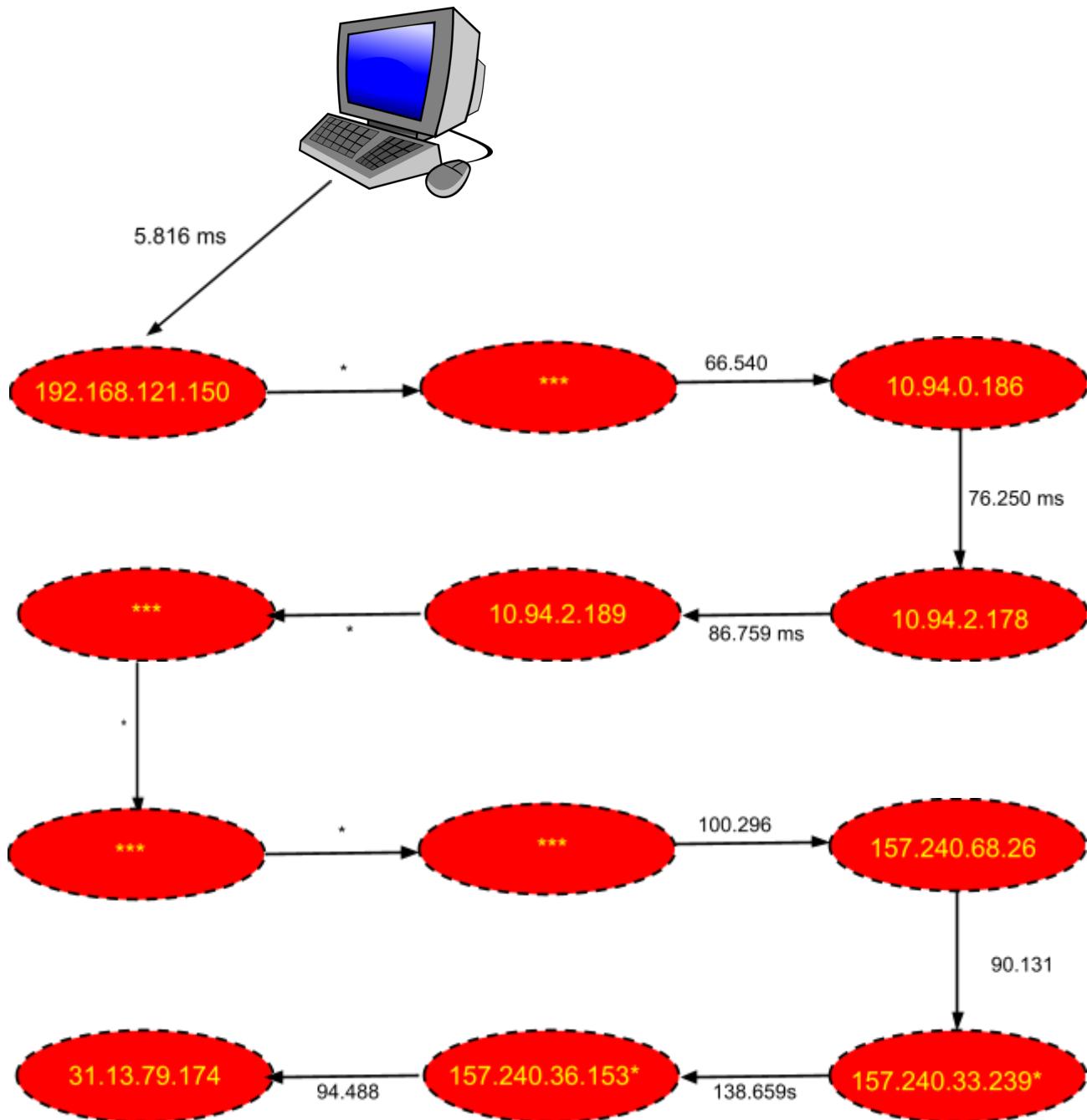
2] www.jiomart.com

Here I am mentioning the RTT of the router at the [x] node on the link joining [x-1] and [x] node. And also this time is RTT of the first packet sent. IP address with * mark having more than one IPs, but i have written only one.

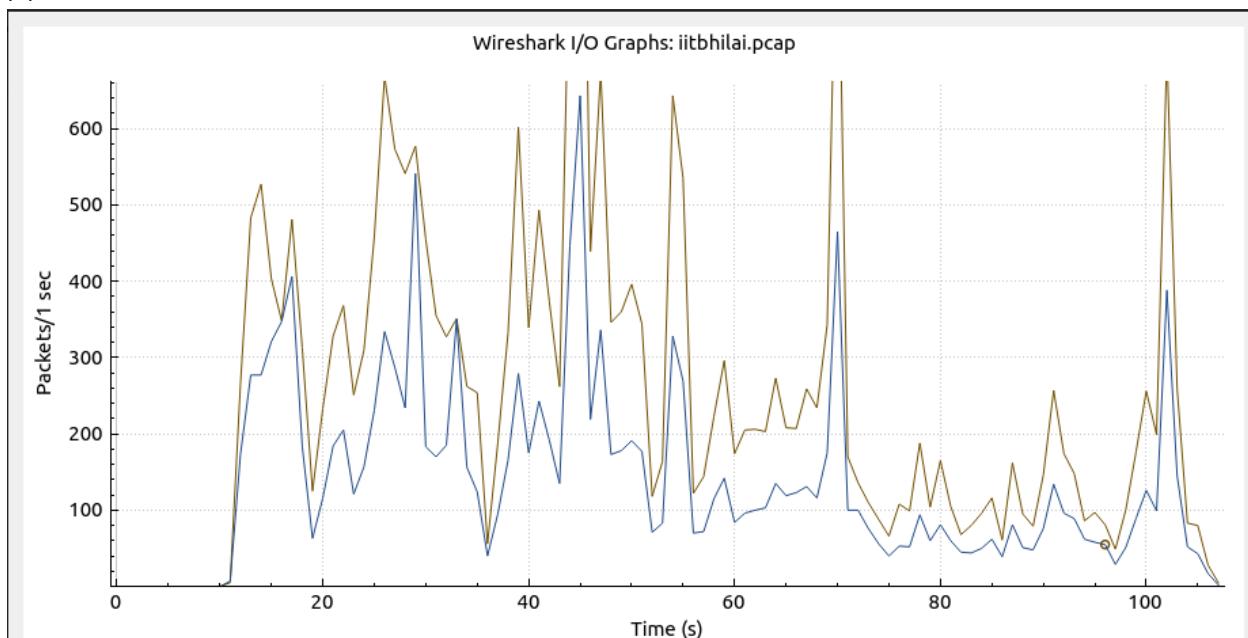


3] www.instagram.com

Here I am mentioning the RTT of the router at the [x] node on the link joining [x-1] and [x] node. And also this time is RTT of the first packet sent. IP address with * mark having more than one IPs, but i have written only one.



(c)



Question 2] Answer

Number	Info	Packet Length(in Bytes)	File Data(in Bytes)
1636	GET / HTTP/1.1	1,226	32853
1697	GET /index.php?pid=css_style HTTP/1.1	2,943	19232
1714	GET /index.php?pid=css_bootstrapmin HTTP/1.1	485	121033
1759	GET /index.php?pid=css_bootstrap_select HTTP/1.1	446	6065
1772	GET /index.php?pid=css_fontawesomemin HTTP/1.1	658	31004
1773	GET /index.php?pid=js_search HTTP/1.1	948	379
1776	GET /index.php?pid=js_bootstrap_select HTTP/1.1	115	31697
1778	GET /index.php?pid=js_jquerymin HTTP/1.1	540	37045
1873	GET /index.php?pid=js_bootstrapmin HTTP/1.1	No Response	No Response
1948	GET /index.php?pid=js_effi_cryptojs HTTP/1.1	734	47944
2056	GET /index.php?pid=js_effi_cryptojs_hmacsha256 HTTP/1.1	879	302
2063	GET /index.php?pid=js_effi_cryptojs_enbase64 HTTP/1.1	439	1100
2129	GET /index.php?pid=js_effi_serviceutility HTTP/1.1	2268	5361

2258	GET /index.php?pid=img_NationalConference HTTP/1.1	1042	384379
2259	GET /index.php?pid=ConstitutionDay HTTP/1.1	No Response	No Response
2260	GET /index.php?pid=unityday_22 HTTP/1.1	No Response	No Response
2261	GET /index.php?pid=orientation HTTP/1.1	No Response	No Response
2269	GET /index.php?pid=director_iitbh HTTP/1.1	No Response	No Response
2306	GET /index.php?pid=img_logo HTTP/1.1	1321	9425
3286	GET /index.php?pid=img_transparent HTTP/1.1	1475	883299
6381	GET /index.php?pid=independence_2023 HTTP/1.1	No Response	No Response
9483	GET /index.php?pid=news1 HTTP/1.1	1077	129366
10589	GET /index.php?pid=news2 HTTP/1.1	No Response	No Response
14588	GET /index.php?pid=news3 HTTP/1.1	No Response	No Response
18384	GET /index.php?pid=favicon HTTP/1.1	No Response	No Response
19908	GET /index.php?pid=img_top_rajiv HTTP/1.1	No Response	No Response
21480	GET /index.php?pid=img_glimpses_pc HTTP/1.1	No Response	No Response
21995	GET /index.php?pid=independence_2022 HTTP/1.1	No Response	No Response
22931	GET /index.php?pid=img_republicday HTTP/1.1	No Response	No Response
23518	GET /index.php?pid=img_HindiPakhwada HTTP/1.1	No Response	No Response
23560	GET /index.php?pid=convocation_carousel HTTP/1.1	No Response	No Response
23737	GET /index.php?pid=img_bhoomipujan HTTP/1.1	No Response	No Response
25642	GET /index.php?pid=img_NEPKiSamajh HTTP/1.1	No Response	No Response
29640	GET /index.php?pid=yoga_2023 HTTP/1.1	No Response	No Response
29986	GET /index.php?pid=img_G20_carousel HTTP/1.1	No Response	No Response
34101	GET /index.php?pid=WorldEnvironmentDay2023 HTTP/1.1	No Response	No Response
35629	GET /index.php?pid=img_smp_2023 HTTP/1.1	No Response	No Response
36086	GET /index.php?pid=img_NationalScienceDay HTTP/1.1	No Response	No Response

Question 3] Answer

(Image in images folder in Part3_Q3 subdirectory)



Last response time is 24.858 ms

22.5518164...	10.10.77.17	14.139.194.5	HTTP	578	3524 GET /templates/iitpatna/images/slidergallery.jpg HTTP/1.1
22.6370408...	10.10.77.17	14.139.194.5	HTTP	569	3581 GET /templates/iitpatna/images/logo.png HTTP/1.1
22.7238315...	10.10.77.17	14.139.194.5	HTTP	590	3647 GET /templates/iitpatna/images/massage-banner_13-09-2021.png
22.7495943...	14.139.194.5	10.10.77.17	HTTP	1559	3664 HTTP/1.1 200 OK
22.7497153...	10.10.77.17	14.139.194.5	HTTP	553	3666 GET /images/a-minus.png HTTP/1.1
22.8289729...	10.10.77.17	14.139.194.5	HTTP	547	3766 GET /images/a.png HTTP/1.1
22.8453005...	14.139.194.5	10.10.77.17	HTTP	2162	3785 HTTP/1.1 200 OK (JPEG/JFIF image)
22.8454470...	10.10.77.17	14.139.194.5	HTTP	549	3789 GET /images/AII.jpg HTTP/1.1
22.8462958...	14.139.194.5	10.10.77.17	HTTP	1472	3790 HTTP/1.1 200 OK (PNG)
22.8464281...	10.10.77.17	14.139.194.5	HTTP	563	3792 GET /images/example-slide-333.jpg HTTP/1.1
22.9125157...	10.10.77.17	14.139.194.5	HTTP	561	3816 GET /images/example-slide-1.jpg HTTP/1.1
23.0046468...	10.10.77.17	14.139.194.5	HTTP	551	3905 GET /images/coe_1.png HTTP/1.1
23.0892084...	14.139.194.5	10.10.77.17	HTTP	1920	3946 HTTP/1.1 200 OK
23.0895182...	10.10.77.17	14.139.194.5	HTTP	556	3948 GET /images/Dron_flag2.jpg HTTP/1.1
23.1273027...	14.139.194.5	10.10.77.17	HTTP	1109	4120 HTTP/1.1 200 OK (JPEG/JFIF image)
23.1274093...	10.10.77.17	14.139.194.5	HTTP	556	4122 GET /images/Dron_flag1.jpg HTTP/1.1
23.7286437...	10.10.77.17	14.139.194.5	HTTP	553	5780 GET /images/favicon.ico HTTP/1.1
23.9002141...	14.139.194.5	10.10.77.17	HTTP	1849	6074 HTTP/1.1 200 OK (image/vnd.microsoft.icon)
24.8582646...	14.139.194.5	10.10.77.17	HTTP	265	7768 HTTP/1.1 200 OK (JPEG/JFIF image)

The page loaded in 6.755 milliseconds, which is the time elapsed between sending the first request from the client to the server and receiving the last response from the server to the client.

(b) 8 connections are used to download this page. We can see all this in Static and then in Conversations part by applying display filters

(c) 23 objects have been transferred between these connections which can be calculated by applying filter "ip.addr == 14.139.194.5 and http.response" in Wireshark. Where given ip address of website of IIT Patna

(d) GET /images/example-slide-16.jpg this Object request take longest time among all request which is 2.412 ms among all objects

DNS

Question 1] Solution

Part 1] Answer

(a) List of all root-server

We can list names of all root server by command `dig NS +short`

Where options are

- `NS` -> Name Server
- `+short` -> Provide short name or terse answer

```
karan@karan-Inspiron-15-3511:~$ dig NS +short
c.root-servers.net.
f.root-servers.net.
k.root-servers.net.
b.root-servers.net.
l.root-servers.net.
i.root-servers.net.
m.root-servers.net.
j.root-servers.net.
h.root-servers.net.
g.root-servers.net.
a.root-servers.net.
e.root-servers.net.
d.root-servers.net.
```

(b) let's find the IP address of www.iitbhilai.ac.in without recursion by dig command

➤ Step 1: find the all root server names by command `dig NS +short`

```
karan@karan-Inspiron-15-3511:~$ dig NS +short
c.root-servers.net.
f.root-servers.net.
k.root-servers.net.
b.root-servers.net.
l.root-servers.net.
i.root-servers.net.
m.root-servers.net.
j.root-servers.net.
h.root-servers.net.
g.root-servers.net.
a.root-servers.net.
e.root-servers.net.
d.root-servers.net.
```

- Step 2 : Request IP Address from first root server, let take ‘c.root-servers.net’ by command (from output of step 1)

```
dig @c.root-servers.net www.iitbihilai.ac.in NS +norecurse
```

```
karan@karan-Inspiron-15-3511:~$ dig @c.root-servers.net www.iitbihilai.ac.in NS +norecurse
; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @c.root-servers.net www.iitbihilai.ac.in NS +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25871
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9a3354448d1763a90100000064f0e361c8b7da02c399c96a (good)
;; QUESTION SECTION:
;www.iitbihilai.ac.in.      IN      NS

;; AUTHORITY SECTION:
in.          172800  IN      NS      ns6.registry.in.
in.          172800  IN      NS      ns3.registry.in.
in.          172800  IN      NS      ns4.registry.in.
in.          172800  IN      NS      ns1.registry.in.
in.          172800  IN      NS      ns2.registry.in.
in.          172800  IN      NS      ns5.registry.in.

;; ADDITIONAL SECTION:
ns6.registry.in.    172800  IN      A      156.154.101.20
ns5.registry.in.    172800  IN      A      156.154.100.20
ns4.registry.in.    172800  IN      A      37.209.198.12
ns3.registry.in.    172800  IN      A      37.209.196.12
ns2.registry.in.    172800  IN      A      37.209.194.12
ns1.registry.in.    172800  IN      A      37.209.192.12
ns6.registry.in.    172800  IN      AAAA   2001:502:ad09::20
ns5.registry.in.    172800  IN      AAAA   2001:502:2eda::20
ns4.registry.in.    172800  IN      AAAA   2001:dcd:4::12
ns3.registry.in.    172800  IN      AAAA   2001:dcd:3::12
ns2.registry.in.    172800  IN      AAAA   2001:dcd:2::12
ns1.registry.in.    172800  IN      AAAA   2001:dcd:1::12

;; Query time: 231 msec
;; SERVER: 192.33.4.12#53(c.root-servers.net) (UDP)
;; WHEN: Fri Sep 01 00:30:49 IST 2023
;; MSG SIZE  rcvd: 461
```

- Step 3 : Now we can request from top level domain, let take ‘ns3.registry.in’ by command(from output of step 2)

```
karan@karan-Inspiron-15-3511:~$ dig @ns1.registry.in www.iitbihilai.ac.in NS +norecurse
; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @ns1.registry.in www.iitbihilai.ac.in NS +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8798
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.iitbihilai.ac.in.      IN      NS

;; AUTHORITY SECTION:
iitbihilai.ac.in.    3600   IN      NS      dns1.iitbihilai.ac.in.
iitbihilai.ac.in.    3600   IN      NS      dns2.iitbihilai.ac.in.

;; ADDITIONAL SECTION:
dns2.iitbihilai.ac.in. 3600   IN      A      103.147.138.111
dns1.iitbihilai.ac.in. 3600   IN      A      103.147.138.110

;; Query time: 55 msec
;; SERVER: 37.209.192.12#53(ns1.registry.in) (UDP)
;; WHEN: Fri Sep 01 00:33:17 IST 2023
;; MSG SIZE  rcvd: 118
```

```
dig @ns1.registry.in www.iitbihilai.ac.in NS +norecurse
```

- Step 4 : Now we can request from DNS server, let take ‘dns2.iitbihilai.ac.in’ by command

```
dig @dns2.iitbihilai.ac.in www.iitbihilai.ac.in A +norecurse
```

```
karan@karan-Inspiron-15-3511:~$ dig @dns2.registry.in www.iitbihilai.ac.in NS +norecurse
dig: couldn't get address for 'dns2.registry.in': not found
```

This indicates that the DNS resolver we are using is unable to resolve the IP address for the DNS server ‘dns2.iitbihilai.ac.in’. So we have to request remaining one DNS server which is ‘dns1.iitbihilai.ac.in’ by command

```
dig @dns1.iitbihilai.ac.in www.iitbihilai.ac.in A +norecurse
```

```
karan@karan-Inspiron-15-3511:~$ dig @dns1.iitbihilai.ac.in www.iitbihilai.ac.in A +norecurse
; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @dns1.iitbihilai.ac.in www.iitbihilai.ac.in A +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4711
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.iitbihilai.ac.in.      IN      A
;;
;; ANSWER SECTION:
www.iitbihilai.ac.in.    10800   IN      A      103.147.138.100
;;
;; AUTHORITY SECTION:
iitbihilai.ac.in.        10800   IN      NS      dns1.iitbihilai.ac.in.
;;
;; ADDITIONAL SECTION:
dns1.iitbihilai.ac.in.   10800   IN      A      103.147.138.110
;;
;; Query time: 67 msec
;; SERVER: 103.147.138.110#53(dns1.iitbihilai.ac.in) (UDP)
;; WHEN: Fri Sep 01 00:42:40 IST 2023
;; MSG SIZE  rcvd: 99
```

And finally we get IP address of our website as **103.147.138.100** as mentioned in below screenshot

(C) List of all servers involved to find IP address of the www.iitbihilai.ac.in

1. **c.root-servers.net**: Root Server
2. **ns4.registry.in**: Top-Level Domain (TLD) Name Server for **.in**
3. **dns1.iitbhilai.ac.in**: Authoritative Name Server for **iitbhilai.ac.in**

(d) let's do this same exercise for other two websites

1. www.google.com

We can start from any root-server let's take '**a.root-servers.net**', so we can get IP of website as follows

➤ **Step 1:**

```
karan@karan-Inspiron-15-3511:~$ dig @a.root-servers.net www.google.com NS -norecur

; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @a.root-servers.net www.google.com NS -norecur
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61520
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.google.com.           IN      NS

;; AUTHORITY SECTION:
com.          172800  IN      NS      a.gtld-servers.net.
com.          172800  IN      NS      b.gtld-servers.net.
com.          172800  IN      NS      c.gtld-servers.net.
com.          172800  IN      NS      d.gtld-servers.net.
com.          172800  IN      NS      e.gtld-servers.net.
com.          172800  IN      NS      f.gtld-servers.net.
com.          172800  IN      NS      g.gtld-servers.net.
com.          172800  IN      NS      h.gtld-servers.net.
com.          172800  IN      NS      i.gtld-servers.net.
com.          172800  IN      NS      j.gtld-servers.net.
com.          172800  IN      NS      k.gtld-servers.net.
com.          172800  IN      NS      l.gtld-servers.net.
com.          172800  IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800  IN      A      192.5.6.30
b.gtld-servers.net. 172800  IN      A      192.33.14.30
c.gtld-servers.net. 172800  IN      A      192.26.92.30
d.gtld-servers.net. 172800  IN      A      192.31.80.30
e.gtld-servers.net. 172800  IN      A      192.12.94.30
f.gtld-servers.net. 172800  IN      A      192.35.51.30
g.gtld-servers.net. 172800  IN      A      192.42.93.30
h.gtld-servers.net. 172800  IN      A      192.54.112.30
i.gtld-servers.net. 172800  IN      A      192.43.172.30
j.gtld-servers.net. 172800  IN      A      192.48.79.30
k.gtld-servers.net. 172800  IN      A      192.52.178.30
l.gtld-servers.net. 172800  IN      A      192.41.162.30
m.gtld-servers.net. 172800  IN      A      192.55.83.30
a.gtld-servers.net. 172800  IN      AAAA    2001:503:a83e::2:30
b.gtld-servers.net. 172800  IN      AAAA    2001:503:231d::2:30
c.gtld-servers.net. 172800  IN      AAAA    2001:503:83eb::30
d.gtld-servers.net. 172800  IN      AAAA    2001:500:856e::30
e.gtld-servers.net. 172800  IN      AAAA    2001:502:1ca1::30
f.gtld-servers.net. 172800  IN      AAAA    2001:503:d414::30
g.gtld-servers.net. 172800  IN      AAAA    2001:503:eea3::30
h.gtld-servers.net. 172800  IN      AAAA    2001:502:8cc::30
```

➤ Step 2

```
karan@karan-Inspiron-15-3511:~$ dig @a.gtld-servers.net www.google.com NS -norecur

; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @a.gtld-servers.net www.google.com NS -norecur
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6476
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.           IN      NS

;; AUTHORITY SECTION:
google.com.          172800  IN      NS      ns2.google.com.
google.com.          172800  IN      NS      ns1.google.com.
google.com.          172800  IN      NS      ns3.google.com.
google.com.          172800  IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.      172800  IN      AAAA    2001:4860:4802:34::a
ns2.google.com.      172800  IN      A       216.239.34.10
ns1.google.com.      172800  IN      AAAA    2001:4860:4802:32::a
ns1.google.com.      172800  IN      A       216.239.32.10
ns3.google.com.      172800  IN      AAAA    2001:4860:4802:36::a
ns3.google.com.      172800  IN      A       216.239.36.10
ns4.google.com.      172800  IN      AAAA    2001:4860:4802:38::a
ns4.google.com.      172800  IN      A       216.239.38.10

;; Query time: 19 msec
;; SERVER: 192.5.6.30#53(a.gtld-servers.net) (UDP)
;; WHEN: Wed Aug 30 01:07:40 IST 2023
;; MSG SIZE rcvd: 291
```

➤ Step 3

```
karan@karan-Inspiron-15-3511:~$ dig @ns2.google.com www.google.com A -norecur

; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @ns2.google.com www.google.com A -norecur
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64963
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.        300     IN      A      142.250.192.68

;; Query time: 91 msec
;; SERVER: 216.239.34.10#53(ns2.google.com) (UDP)
;; WHEN: Wed Aug 30 01:09:12 IST 2023
;; MSG SIZE rcvd: 59

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 30128
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
```

List of all servers involved to find IP address of the www.wikipedia.com

1. **a.root-servers.net**
2. **a.gtld--servers.net**
3. **ns2.google.com**

IP Address :- 142.250.192.68

2. www.gnu.org

We can start from any root-server let's take '**b.root-servers.net**', so we can get IP of website as follows

➤ Step 1

```
karan@karan-Inspiron-15-3511:~$ dig @b.root-servers.net www.gnu.org NS -norecur

; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @b.root-servers.net www.gnu.org NS -norecur
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46706
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.gnu.org.           IN      NS

;; AUTHORITY SECTION:
org.                  172800  IN      NS      a0.org.afiliias-nst.info.
org.                  172800  IN      NS      a2.org.afiliias-nst.info.
org.                  172800  IN      NS      b0.org.afiliias-nst.org.
org.                  172800  IN      NS      b2.org.afiliias-nst.org.
org.                  172800  IN      NS      c0.org.afiliias-nst.info.
org.                  172800  IN      NS      d0.org.afiliias-nst.org.

;; ADDITIONAL SECTION:
b0.org.afiliias-nst.org. 172800  IN      A       199.19.54.1
b0.org.afiliias-nst.org. 172800  IN      AAAA    2001:500:c::1
b2.org.afiliias-nst.org. 172800  IN      A       199.249.120.1
b2.org.afiliias-nst.org. 172800  IN      AAAA    2001:500:48::1
d0.org.afiliias-nst.org. 172800  IN      A       199.19.57.1
d0.org.afiliias-nst.org. 172800  IN      AAAA    2001:500:f::1
a0.org.afiliias-nst.info. 172800 IN      A       199.19.56.1
a0.org.afiliias-nst.info. 172800 IN      AAAA    2001:500:e::1
a2.org.afiliias-nst.info. 172800 IN      A       199.249.112.1
a2.org.afiliias-nst.info. 172800 IN      AAAA    2001:500:40::1
c0.org.afiliias-nst.info. 172800 IN      A       199.19.53.1
c0.org.afiliias-nst.info. 172800 IN      AAAA    2001:500:b::1

;; Query time: 80 msec
;; SERVER: 199.9.14.201#53(b.root-servers.net) (UDP)
;; WHEN: Wed Aug 30 01:26:38 IST 2023
;; MSG SIZE  rcvd: 484
```

➤ Step 2

```
karan@karan-Inspiron-15-3511:~$ dig @a0.org.afilias-nst.info www.gnu.org NS -norecur

; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @a0.org.afilias-nst.info www.gnu.org NS -norecur
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 33410
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.gnu.org.           IN      NS

;; AUTHORITY SECTION:
gnu.org.          3600    IN      NS      ns1.gnu.org.
gnu.org.          3600    IN      NS      ns3.gnu.org.
gnu.org.          3600    IN      NS      ns2.gnu.org.
gnu.org.          3600    IN      NS      ns4.gnu.org.

;; ADDITIONAL SECTION:
ns1.gnu.org.       3600    IN      A       192.99.37.66
ns2.gnu.org.       3600    IN      A       192.99.35.98
ns3.gnu.org.       3600    IN      A       185.199.142.2
ns4.gnu.org.       3600    IN      A       188.165.235.157
ns1.gnu.org.       3600    IN      AAAA   2607:5300:60:4c42::1
ns2.gnu.org.       3600    IN      AAAA   2607:5300:60:4a62::1
ns4.gnu.org.       3600    IN      AAAA   2001:41d0:2:b69d::1

;; Query time: 99 msec
;; SERVER: 199.19.56.1#53(a0.org.afilias-nst.info) (UDP)
;; WHEN: Wed Aug 30 01:27:16 IST 2023
;; MSG SIZE rcvd: 260

;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: REFUSED, id: 6859
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

➤ Step 3

```
karan@karan-Inspiron-15-3511:~$ dig @ns1.gnu.org www.gnu.org A -norecur

; <>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <>> @ns1.gnu.org www.gnu.org A -norecur
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35079
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a140196d2a72db4a0100000064ee4dc12b5481bbb3ddbac3 (good)
;; QUESTION SECTION:
;www.gnu.org.           IN      A

;; ANSWER SECTION:
www.gnu.org.        1800    IN      A      209.51.188.116

;; Query time: 331 msec
;; SERVER: 192.99.37.66#53(ns1.gnu.org) (UDP)
;; WHEN: Wed Aug 30 01:27:53 IST 2023
;; MSG SIZE rcvd: 84

;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: REFUSED, id: 27390
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

List of all servers involved to find IP address of the www.gnu.org

4. b.root-servers.net
5. a0.org.afilias-nst.info
6. ns1.gnu.org

IP Address :- 209.51.188.116