

Computer Networks Assignment - 1

Shivam Agarwal CSE-2020123

Ans 1.(a) The ip address of my network interface using ipconfig(Windows) is : 192.168.54.195

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : iiitd.edu.in
Description . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
Physical Address. . . . . : AC-12-03-3D-19-9F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::78cc:5514:4988:84cc%13(Preferred)
IPv4 Address. . . . . : 192.168.54.195(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Lease Obtained. . . . . : 21 September 2022 09:37:55
Lease Expires . . . . . : 30 September 2022 21:48:55
Default Gateway . . . . . : 192.168.48.11
DHCP Server . . . . . : 192.168.1.7
DHCPv6 IAID . . . . . : 111940099
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-59-B4-EE-AC-12-03-3D-19-9F
DNS Servers . . . . . : 192.168.1.8
                        192.168.1.7
NetBIOS over Tcpi. . . . . : Enabled
```

Ans 1.(b) My Ip address using whatismyip.com is 180.151.15.242 .
Which is different from the one found using ipconfig. The reason behind this is that there are a limited number of ip addresses in the world so we use NAT or Network Address Translation to map our ip address to another.

Host Info for 180.151.15.242

ISP: Shyam Spectra Pvt Ltd

Domain: spectranet.in

Network Speed: DSL

180.151.15.242 - ip address on
whatismyip.com

Ans 2.(a)

```
C:\>nslookup -type=soa google.com
Server: ns3.iiitd.edu.in
Address: 192.168.1.8

Non-authoritative answer:
google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial = 475782946
    refresh = 900 (15 mins)
    retry = 900 (15 mins)
    expire = 1800 (30 mins)
    default TTL = 60 (1 min)

ns1.google.com internet address = 216.239.32.10
ns1.google.com AAAA IPv6 address = 2001:4860:4802:32::a

C:\>nslookup google.com ns1.google.com
Server: ns1.google.com
Address: 216.239.32.10

Name: google.com
Addresses: 2404:6800:4002:805::200e
           216.58.196.206
```

First we get the name of the authoritative DNS server. To do this we use type=soa (i.e Start of Authority). Then we query the authoritative DNS server to get the authoritative response.

Ans 2.(b) We can see that the default TTL(Time To Live) of the dns record of Google.com in the local DNS server is 60 secs i.e 1 minute. So after 1 minute since its refresh this record will expire.

Ans 3.(a)

```
C:\>tracert google.in

Tracing route to google.in [142.250.192.132]
over a maximum of 30 hops:

  1    1 ms    2 ms    2 ms  192.168.48.254
  2    1 ms    6 ms    1 ms  vpn.iiitd.edu.in [192.168.1.99]
  3    1 ms    1 ms    1 ms  180.151.15.241.reverse.spectranet.in [180.151.15.241]
  4    3 ms    3 ms    2 ms  72.14.194.202
  5    6 ms    7 ms    8 ms  108.170.251.108
  6    3 ms    3 ms    4 ms  72.14.233.107
  7   21 ms   21 ms   21 ms  72.14.232.138
  8   22 ms   23 ms   22 ms  108.170.248.161
  9   32 ms   24 ms   24 ms  142.250.238.81
 10   24 ms   24 ms   24 ms  bom12s18-in-f4.1e100.net [142.250.192.132]

Trace complete.
```

We can see that there are 9 intermediate hosts as the 10th host is our destination ip i.e google.in

Average latency for each hop :

IP Address	Average Latency(in ms)
192.168.48.254	1.66
vpn.iiitd.edu.in [192.168.1.99]	2.66
180.151.15.241.reverse.spectranet. in	1
72.14.194.202	2.66
108.170.251.108	7
72.14.233.107	3.33
72.14.232.138	21
108.170.248.161	22.33
142.250.238.81	26.66
bom12s18-in-f4.1e100.net [142.250.192.132]	24

Ans 3.(b)

```
C:\>ping -n 100 google.in

Pinging google.in [216.58.221.36] with 32 bytes of data:
Reply from 216.58.221.36: bytes=32 time=5ms TTL=117
Reply from 216.58.221.36: bytes=32 time=3ms TTL=117
Reply from 216.58.221.36: bytes=32 time=4ms TTL=117
Reply from 216.58.221.36: bytes=32 time=5ms TTL=117
Reply from 216.58.221.36: bytes=32 time=2ms TTL=117
Reply from 216.58.221.36: bytes=32 time=2ms TTL=117
Reply from 216.58.221.36: bytes=32 time=2ms TTL=117
Reply from 216.58.221.36: bytes=32 time=2ms TTL=117
Reply from 216.58.221.36: bytes=32 time=4ms TTL=117
Reply from 216.58.221.36: bytes=32 time=3ms TTL=117
Reply from 216.58.221.36: bytes=32 time=4ms TTL=117
Reply from 216.58.221.36: bytes=32 time=3ms TTL=117

Ping statistics for 216.58.221.36:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 22ms, Average = 2ms
```

So avg time for each ping = 2ms

Ans 3.(c)

```
C:\>ping -n 100 columbia.edu

Pinging columbia.edu [128.59.105.24] with 32 bytes of data:
Reply from 128.59.105.24: bytes=32 time=246ms TTL=234
Reply from 128.59.105.24: bytes=32 time=243ms TTL=234
Reply from 128.59.105.24: bytes=32 time=242ms TTL=234
Reply from 128.59.105.24: bytes=32 time=242ms TTL=234
Reply from 128.59.105.24: bytes=32 time=242ms TTL=234
```

```
Reply from 128.59.105.24: bytes=32 time=241ms TTL=234
Reply from 128.59.105.24: bytes=32 time=242ms TTL=234
Reply from 128.59.105.24: bytes=32 time=241ms TTL=234
Reply from 128.59.105.24: bytes=32 time=242ms TTL=234
Reply from 128.59.105.24: bytes=32 time=253ms TTL=234

Ping statistics for 128.59.105.24:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 241ms, Maximum = 253ms, Average = 241ms
```

So average time for each ping is 241ms

Ans 3.(d) No, they are not matching. We get a larger latency when we sum all the intermediate latencies than compared to the one in the (b) part. Reason for this is that the tracert command gets the latency for each node in the route from the host. That means in the later nodes, latency of the previous nodes is already accounted for.

Ans 3.(e) No, they are not matching. A cause of this can be that routers tend to prioritize packet forwarding. So it forwards the ping request quickly but takes time to give back response to the host in case of tracert. This time makes the response from tracert to have higher latency.

Ans 3.(f)

```
C:\>tracert columbia.edu

Tracing route to columbia.edu [128.59.105.24]
over a maximum of 30 hops:

  1    2 ms    4 ms    1 ms  192.168.48.254
  2    1 ms    1 ms    1 ms  auth.iiitd.edu.in [192.168.1.99]
  3    2 ms    2 ms    2 ms  180.151.15.241.reverse.spectranet.in [180.151.15.241]
  4    6 ms    3 ms    4 ms  219.65.112.205.static-delhi.vsnl.net.in [219.65.112.205]
  5   23 ms   23 ms   24 ms  172.23.183.134
  6  406 ms   25 ms   25 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7    *      *      *      Request timed out.
  8    *      *      *      Request timed out.
  9   146 ms  144 ms  145 ms  if-ae-55-4.tcore1.pvu-paris.as6453.net [80.231.153.168]
 10   141 ms  141 ms  141 ms  be6453.agr21.par04.atlas.cogentco.com [130.117.15.69]
 11   148 ms  145 ms  197 ms  be2151.ccr32.par04.atlas.cogentco.com [154.54.61.33]
 12   146 ms  146 ms  145 ms  be2103.ccr42.par01.atlas.cogentco.com [154.54.61.21]
 13   238 ms  238 ms  238 ms  be3628.ccr42.jfk02.atlas.cogentco.com [154.54.27.169]
 14   238 ms  238 ms  237 ms  be2897.rcr24.jfk01.atlas.cogentco.com [154.54.84.214]
 15   237 ms  236 ms  237 ms  38.122.8.210
 16   240 ms  241 ms  240 ms  cc-core-1-x-nyser32-gw-1.net.columbia.edu [128.59.255.5]
 17   237 ms  236 ms  238 ms  cc-conc-1-x-cc-core-1.net.columbia.edu [128.59.255.21]
 18   243 ms  242 ms  243 ms  www-ltm.cc.columbia.edu [128.59.105.24]

Trace complete.
```

Google.in takes 10 hops whereas Columbia.edu takes 18 hops. Latency difference between the two is due to the fact that for columbia.edu, we have to travel a large distance which adds a high propagation delay in packet transmission.

Ans 4. We can make the ping command to 127.0.0.1 fail with a 100% packet loss by turning down the local host using the command :

Sudo Ifconfig lo down

(I am not able to put a screenshot because windows doesn't allow you to access with the local host using cmd)

Ans 5.

No.	Time	Source	Destination	Protocol	Length	Info
342	17.368180	192.168.1.66	188.184.21.108	HTTP	524	GET / HTTP/1.1
344	17.611389	188.184.21.108	192.168.1.66	HTTP	932	HTTP/1.1 200 OK (text/html)
348	17.668181	192.168.1.66	188.184.21.108	HTTP	465	GET /favicon.ico HTTP/1.1
357	17.860868	188.184.21.108	192.168.1.66	HTTP	296	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

Part 1:

```
▼ Hypertext Transfer Protocol
  ▼ GET / HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      [GET / HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: info.cern.ch\r\n
      Connection: keep-alive\r\n
      Pragma: no-cache\r\n
      Cache-Control: no-cache\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      \r\n
      [Full request URI: http://info.cern.ch/]
      [HTTP request 1/1]
      [Response in frame: 344]
```

Request type : GET

User Agent Type : Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36

HTTP request packet's URL : <http://info.cern.ch/>

Part 2:

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Fri, 23 Sep 2022 16:25:30 GMT\r\n
      Server: Apache\r\n
      Last-Modified: Wed, 05 Feb 2014 16:00:31 GMT\r\n
      ETag: "286-4f1aadb3105c0"\r\n
      . . . . .
```

HTTP response code : 200(ok)

HTTP response description : request succeeded, requested object later in this message, with the message being

```
<html><head></head><body><header>\n
<title>http://info.cern.ch</title>\n
</header>\n
\n
<h1>http://info.cern.ch - home of the first website</h1>\n
<p>From here you can:</p>\n
<ul>\n
<li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the first website</a></li>\n
<li><a href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse the first website using the line-mode browser simulator</a></li>\n
<li><a href="http://home.web.cern.ch/topics/birth-web">Learn about the birth of the web</a></li>\n
<li><a href="http://home.web.cern.ch/about">Learn about CERN, the physics laboratory where the web was born</a></li>\n
</ul>\n
</body></html>\n
```

Name and version of the web server : Apache(name) HTTP version 1.1

Part 3:

No.	Time	Source	Destination	Protocol	Length	Info
177	8.810807	188.184.21.108	192.168.1.66	TCP	66	80 → 51578 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412
180	8.830755	188.184.21.108	192.168.1.66	TCP	66	80 → 51579 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412
343	17.611389	188.184.21.108	192.168.1.66	TCP	54	80 → 51578 [ACK] Seq=1 Ack=471 Win=30336 Len=0
344	17.611389	188.184.21.108	192.168.1.66	HTTP	932	HTTP/1.1 200 OK (text/html)
345	17.611389	188.184.21.108	192.168.1.66	TCP	54	80 → 51578 [FIN, ACK] Seq=879 Ack=471 Win=30336 Len=0
352	17.775089	188.184.21.108	192.168.1.66	TCP	54	80 → 51578 [ACK] Seq=880 Ack=472 Win=30336 Len=0
355	17.855911	188.184.21.108	192.168.1.66	TCP	54	80 → 51579 [ACK] Seq=1 Ack=412 Win=30336 Len=0
356	17.860868	188.184.21.108	192.168.1.66	TCP	1466	80 → 51579 [ACK] Seq=1 Ack=412 Win=30336 Len=1412 [TCP seg...
357	17.860868	188.184.21.108	192.168.1.66	HTTP	296	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
358	17.860868	188.184.21.108	192.168.1.66	TCP	54	80 → 51579 [FIN, ACK] Seq=1655 Ack=412 Win=30336 Len=0
364	18.054773	188.184.21.108	192.168.1.66	TCP	54	80 → 51579 [ACK] Seq=1656 Ack=413 Win=30336 Len=0

e	Destination	Protocol	Length	Info	port	des port
184.21.108	192.168.1.66	TCP	66	80 → 51578 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PE...	80	51578
184.21.108	192.168.1.66	TCP	66	80 → 51579 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PE...	80	51579
184.21.108	192.168.1.66	TCP	54	80 → 51578 [ACK] Seq=1 Ack=471 Win=30336 Len=0	80	51578
184.21.108	192.168.1.66	HTTP	932	HTTP/1.1 200 OK (text/html)	80	51578
184.21.108	192.168.1.66	TCP	54	80 → 51578 [FIN, ACK] Seq=879 Ack=471 Win=30336 Len=0	80	51578
184.21.108	192.168.1.66	TCP	54	80 → 51578 [ACK] Seq=880 Ack=472 Win=30336 Len=0	80	51578
184.21.108	192.168.1.66	TCP	54	80 → 51579 [ACK] Seq=1 Ack=412 Win=30336 Len=0	80	51579
184.21.108	192.168.1.66	TCP	1466	80 → 51579 [ACK] Seq=1 Ack=412 Win=30336 Len=1412 [TCP segment of ...	80	51579
184.21.108	192.168.1.66	HTTP	296	HTTP/1.1 200 OK (image/vnd.microsoft.icon)	80	51579
184.21.108	192.168.1.66	TCP	54	80 → 51579 [FIN, ACK] Seq=1655 Ack=412 Win=30336 Len=0	80	51579
184.21.108	192.168.1.66	TCP	54	80 → 51579 [ACK] Seq=1656 Ack=413 Win=30336 Len=0	80	51579

From this we can see that the entire web page was sent over only 1 TCP connection and the rest of the TCP connections have 0 length

Part 4: From the above we can say that the connection is persistent

Ans 6.(a) For Windows :

Netstat -a -p TCP

-a : to give all connections

-p TCP : to give TCP connections

Ans 6.(b) The TCP connection has been closed because we can't find the given connection using netstat command. So it must have terminated.