160118737084
Srija Chitikesi

CN Assignment -1

1) Simple tools for troubleshooting TCP/IP network

1: -n 5 Option sets the number of ICMP echo requests to send, from 1 to 4294967295. The ping command will send 4 by default if -n isn't used.

2. The average value of the RTT obtained is 267ms

Round time trip is the length time it takes for a data packet to be sent to a destination plus the time it takes for an acknowledgement of that packet to be received back at the origin. The average time taken by the requests is calculated and it is known as the average value of RTT.

3. The value of TTL Obtained is

Time to live is a value in an internet protocol packet that tells a network router whether or not the packet has been in the network too long and should be discarded.

2) Use the traceroute program to find the paths

destination address - www.google.com [2404:6800:4007:815::2004]

Number of hops - maximum 30 hops

Ip addres of five nodes where there is maximum delay and the delay experienced on these hops

1	13ms	6ms	11ms	2405:203:400:100:172:31:2:15
9	21ms	17ms	17ms	2405:200:801:960::1
3	33ms	25ms	69ms	2001:4800:1:1:0:da1c:0:16
4	16ms	19ms	15ms	2001:4860:6:1355:1
5	42ms	26ms	21ms	2001:4860:0:1:565

2. nslookup -

The domain name of the DNS server you have used - [illegible]

The IP address obtained - 2405:201:6011:8998:[illegible]

working of DNS: Domain name system is one of the foundation of internet. The DNS directory that matches names to numbers isn't located all in one place in one data center in the internet. As centralized DNS do not scale because of the reasons mentioned above, a need arose to implement DNS in a distributed manner. The DNS is a distributed system implemented in a hierarchy of many name servers.

4. netstat -rn

Route Table

IPv4 Route Table

Active Routes

Network destination	Network	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.29.1	192.168.29.43	50
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
192.168.29.0	255.255.255.0	On-link	192.168.29.43	306
192.168.29.43	255.255.255.255	On-link	192.168.29.43	306
192.168.29.255	255.255.255.255	On-link	192.168.29.43	306
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	192.168.29.43	306
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	192.168.29.43	306

Network - The network ID or destination corresponding to the route Subnet Mask - The mask that is used to match a destination IP address to the network ID.

Nexthop - The IP address to which the packet is forwarded.

Outgoing Interface - The packet should go out to reach the destination network.

Metric - used to indicate the minimum number of hops, when a router receives a packet, it examines the destination IP address, and looks up into its routing table to figure out which interface packet will be send out.

5. Netstat? - used to display all the parameters

netstat -n -a

- Transport protocol - TCP
- Local address and port number - 127.0.0.1:49669
- Foreign address - 127.0.0.1:49670
- Remote address - local host:49670
- -o is the command to get the process ID for the connection

UDP & DNS

1. Type Udp in the wireshark text box. you will see multiple packets information

2. a) UDP is the protocol listed

b) No, Time, Source, destination, protocol lengths info

c) 6, 7.376029, 2404:6800:4003:c00::bd, 2405:201:c011:8988:e9fa:
blbe:a196:d39900, 106,
443 → 60269 Len=44

d) A DNS response is based on a query generated for a domain. in the response message NIDS capture the TTL value of resource record, the resource record type be resource data.

TCP

9 a) The Sequence number of the TCPSYN segment which is used to initialize the Tcp connection. between the server and the host is 0. 86 54824 → 443. The SYN flag is set to 1 and it indicates that this segment is SYN segment.

b) The Sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client is 0.

The value of acknowledgement field in the SYNACK segment is 1.

c) The Sequence number of the HTTP post comm and is 1.

d) Sequence numbers Time

Segment 1 is 716 → 0.27125000

Segment 2 is 2164 → 0.27142500

Segment 3 is 3612 → 0.27179700

Segment 4 is 5060 → 0.27179800

Segment 5 is 3612 → 0.36708100

Segment 6 is 5060 → 0.36871100

e, f → Screenshots

g) Congestion avoidance takes over at about 0.7 seconds because it cuts down the amount being sent.

10) Screenshot.

Ip

5. a) The version of the Ip is IpV6.

host - fe80::3248:50ff:fe2b:9643

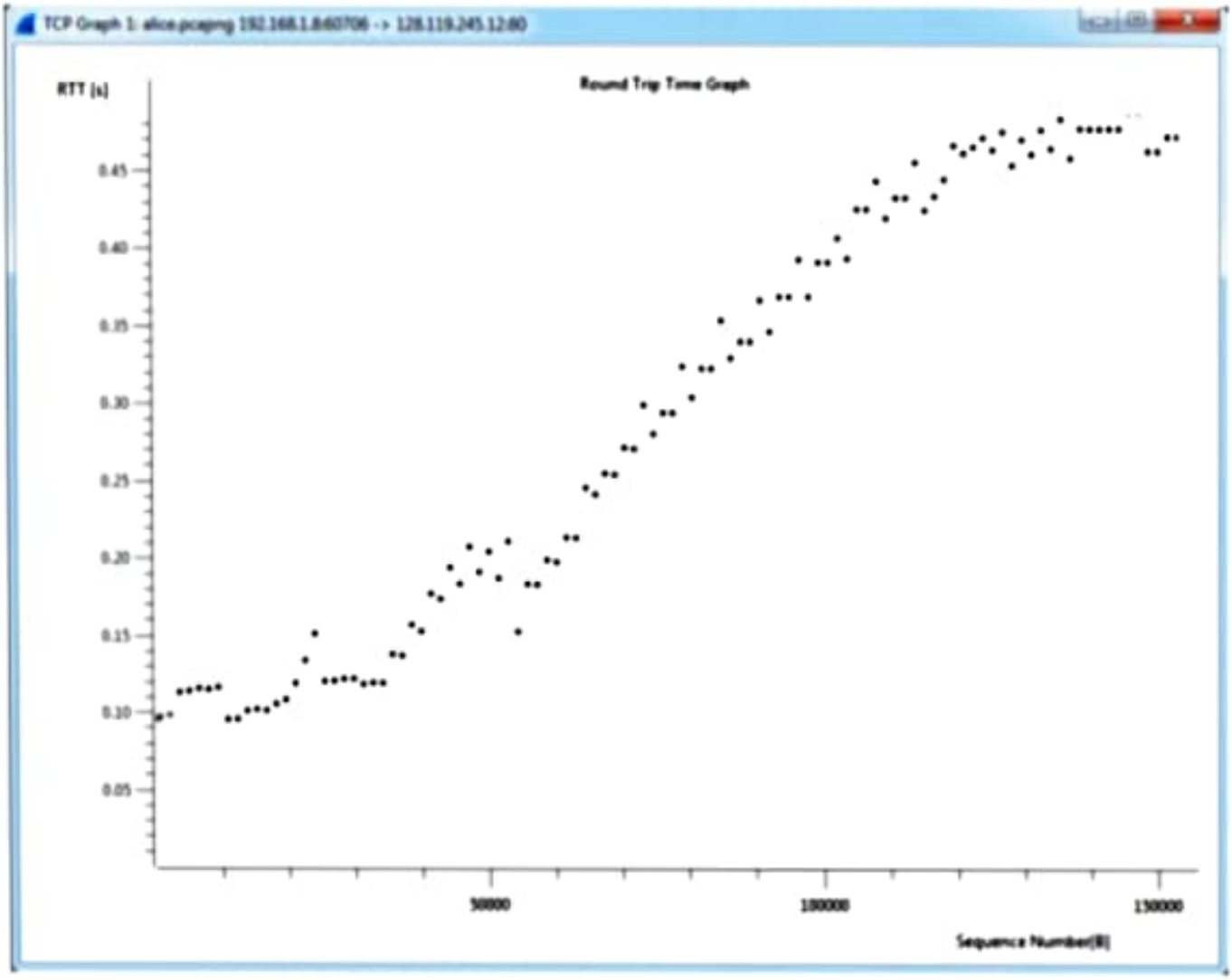
b) within like Ip header the value of the upper layer header is ICMP.

c) The size of the header length is 58 bytes

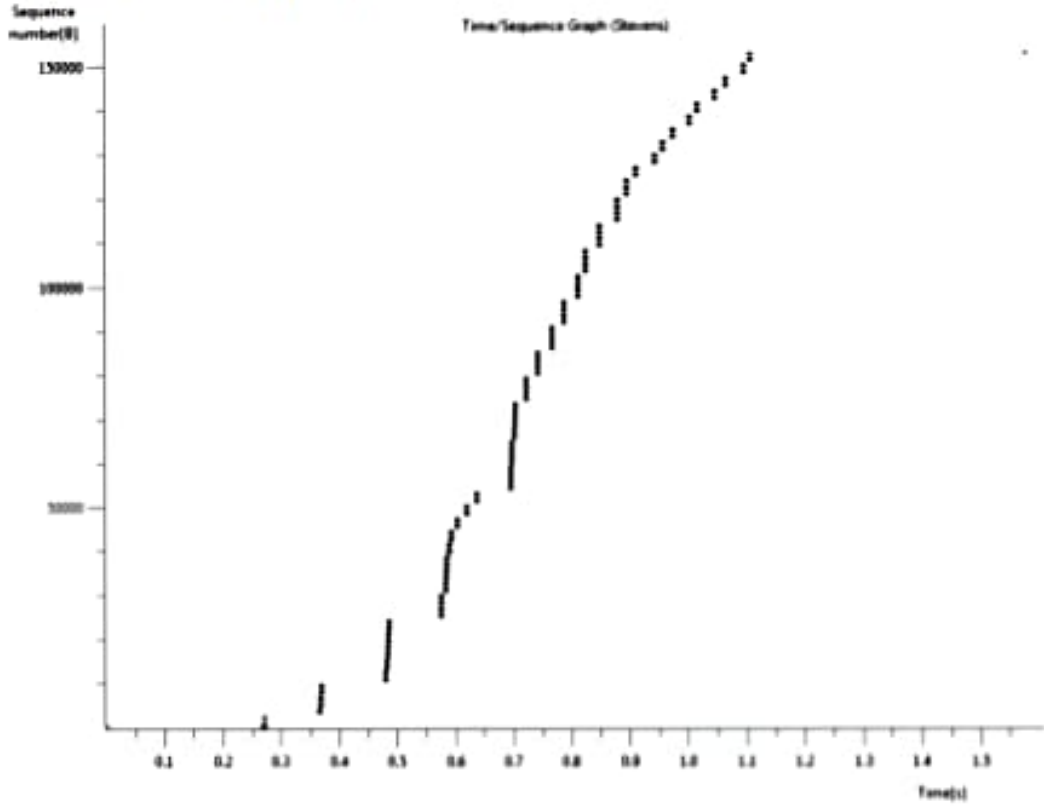
d) The flag fragment is 0. Hence it is not fragmented.

TCP

9.e) round trip time



9 f) time sequence graph (stevens)



10.

```
No.   Time        Source          Destination     Protocol Length Info
    5 0.26860900 192.168.1.8      128.119.245.12  TCP        66 60706 > http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=85
    6 0.27137700 192.168.1.8      128.119.245.12  TCP       644 60706 > http [PSH, ACK] Seq=1 Ack=1 Win=131760 Len=578
    7 0.27142500 192.168.1.8      128.119.245.12  TCP       203 60706 > http [PSH, ACK] Seq=579 Ack=1 Win=131760 Len=137
    8 0.27178700 192.168.1.8      128.119.245.12  TCP      1514 60706 > http [ACK] Seq=716 Ack=1 Win=131760 Len=1448 TSv
    9 0.27179800 192.168.1.8      128.119.245.12  TCP      1514 60706 > http [ACK] Seq=2164 Ack=1 Win=131760 Len=1448 TS
   10 0.36893100 128.119.245.12   192.168.1.8     TCP        66 http > 60706 [ACK] Seq=1 Ack=579 Win=7040 Len=0 TSval=22
   11 0.36708100 192.168.1.8      128.119.245.12  TCP      1514 60706 > http [ACK] Seq=3612 Ack=1 Win=131760 Len=1448 TS
   12 0.36728900 128.119.245.12   192.168.1.8     TCP        66 http > 60706 [ACK] Seq=1 Ack=716 Win=8192 Len=0 TSval=22
   13 0.36861700 128.119.245.12   192.168.1.8     TCP        66 http > 60706 [ACK] Seq=1 Ack=2164 Win=11008 Len=0 TSval=
   14 0.36871100 192.168.1.8      128.119.245.12  TCP      1514 60706 > http [ACK] Seq=5060 Ack=1 Win=131760 Len=1448 TS

⊞ Frame 6: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface 0
⊞ Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
⊞ Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
⊟ Transmission Control Protocol, Src Port: 60706 (60706), Dst Port: http (80), Seq: 1, Ack: 1, Len: 578
    Source port: 60706 (60706)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 579    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header length: 32 bytes
  ⊟ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set

0000  a0 f3 c1 f8 6d f9 b8 e8  56 1f d4 56 08 00 45 00   ....m... V..V..E.
0010  02 76 f0 5a 40 00 40 06  0a f3 c0 a8 01 08 80 77   .v.Z@.@. .......w
0020  f5 0c ed 22 00 50 1f e9  a7 e8 79 47 80 0a 80 18   ...".P.. ..yG....
0030  20 2b bf 08 00 00 01 01  08 0a 05 16 f8 ee 86 ca    +...... ........
0040  ee 56 50 4f 53 54 20 2f  77 69 72 65 73 68 61 72   .vPOST / wireshar
0050  6b 2d 6c 61 62 73 2f 6c  61 62 33 2d 31 2d 72 65   k-labs/l ab3-1-re
0060  70 6c 79 2e 68 74 6d 20  48 54 54 50 2f 31 2e 31   ply.htm  HTTP/1.1
0070  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ..Host:  gaia.cs.
0080  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 74 65   umass.ed u..Conte
0090  6e 74 2d 54 79 70 65 3a  20 6d 75 6c 74 69 70 61   nt-Type:  multipa
00a0  72 74 2f 66 6f 72 6d 2d  64 61 74 61 3b 20 62 6f   rt/form- data; bo
```

IP