NETWORK TOOLS FOR INVESTIGATION AND PERFORMANCE MEASUREMENT

JAYATILAKA G.C.
E/14/118
GROUP 06
SEMESTER 03
31/01/2017

PART-1: NETWORK TOOLS

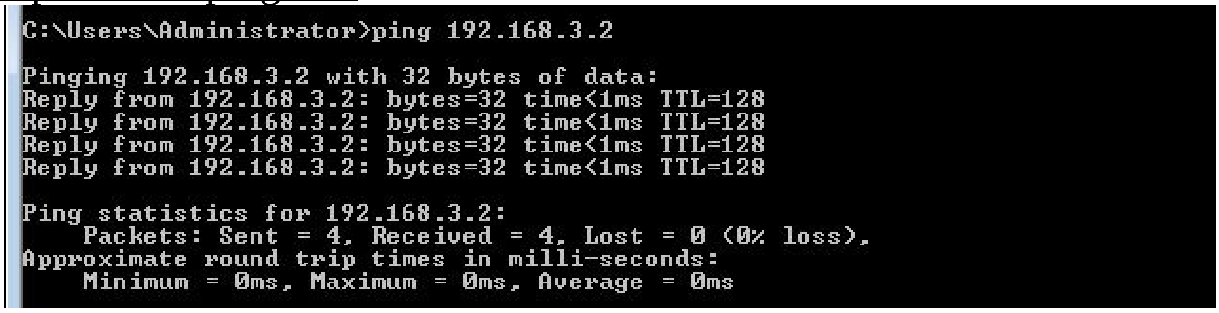
PING

Usefulness:

Ping has two used in an network

1. To check whether a certain ip address could be reached from a device
2. To see the time taken for a data packet to be sent to a certain ip address from a device and to receive it (the total time of the round trip could be obtained)
3. To check whether the data is lost in a network while being transmitted to a certain ip address.

Output of the ping tool



```
C:\Users\Administrator>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The first line of the output shows the ip the ping tool is trying to reach and the amount of data per a packet sent,

The next 4 lines (in windows command prompt ping) shows the time taken by a packet for the round trip from out device to the intended ip. The smallest unit of time measure in windows tool is 1ms. The linux tool shows the time in the scale of 0.001ms and shows the data for packets continuously instead of stopping at 4.

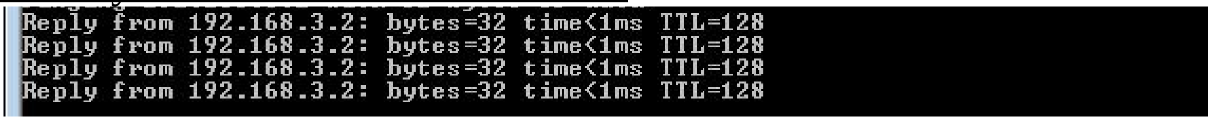
Next the output has a summary of the reliability of the packet transfer. It shows the number of packets sent, received and lost in the transmission. The loss is shown as a percentage as well.

Then the time statistics of the packet transfer is shown. The minimum, maximum and the average time per a single packet’s round trip is shown.

Measuring delay

The type of delay measured in this tool is the time taken for a round trip transfer of a packet of data. This has three components as the time for the transmission to the ip, the time for the packet to be processed and the time for the transmission from the ip to us. The value the tool displays is the sum of all these.

The delay measurement in the network



```
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
```

The delay was less than 1ms during the measure.

TRACEROUTE

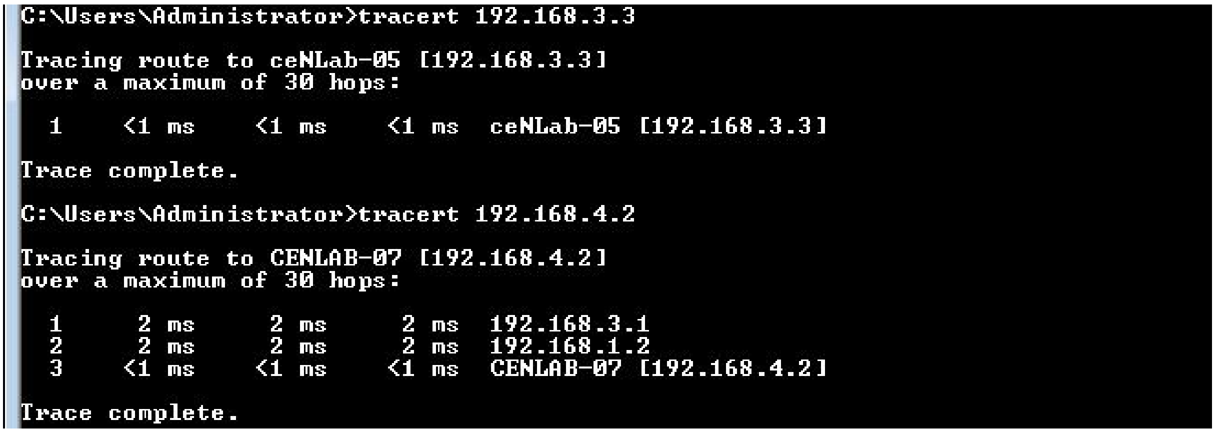
Usefulness

When a packet is sent from the our computer (the source) to another ip (destination) it has to go through a route within the network. The route can be a single cable or through multiple network devices. Traceroute is used to see the path (The ips of the nodes in the path) a packet takes to go to the destination and also to see the round trip time for every node (Instead of having to ping to every node separately).

Difference from ping

Ping gives the round trip time for a packet between the source and the destination. In contrast, traceroute gives he ip addresses of all the devices within the path from the source to destination and also the round trip time in between the source and every node (of the path) seperately.

Output



```
C:\Users\Administrator>tracert 192.168.3.3

Tracing route to ceNLab-05 [192.168.3.3]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  ceNLab-05 [192.168.3.3]

Trace complete.

C:\Users\Administrator>tracert 192.168.4.2

Tracing route to CENLAB-07 [192.168.4.2]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.3.1
  2     2 ms     2 ms     2 ms  192.168.1.2
  3    <1 ms    <1 ms    <1 ms  CENLAB-07 [192.168.4.2]

Trace complete.
```

The first line of the output shows the ip address of the destination device. The next line shows the maximum number of hops (Number of devices in the path – 1) the tool is going to look at in this path.

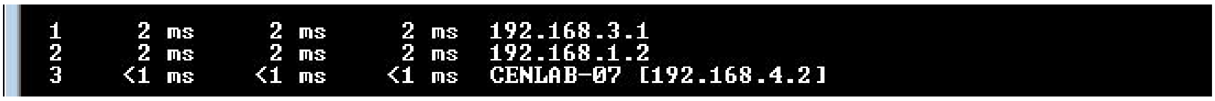
The next few lines have a table consisting of the nodes of the path the packet takes from the source to the destination.

The first column is the position of the ip in the path (1 being the ip of the device adjacent to the source computer). The next three columns are the round trip time from the source to that device and the last column is the ip of the device.

Measuring delay

Traceroute measures the delay for the round trips of data packets from the source to every node in the path to the destination. It takes 3 measurements for a node.

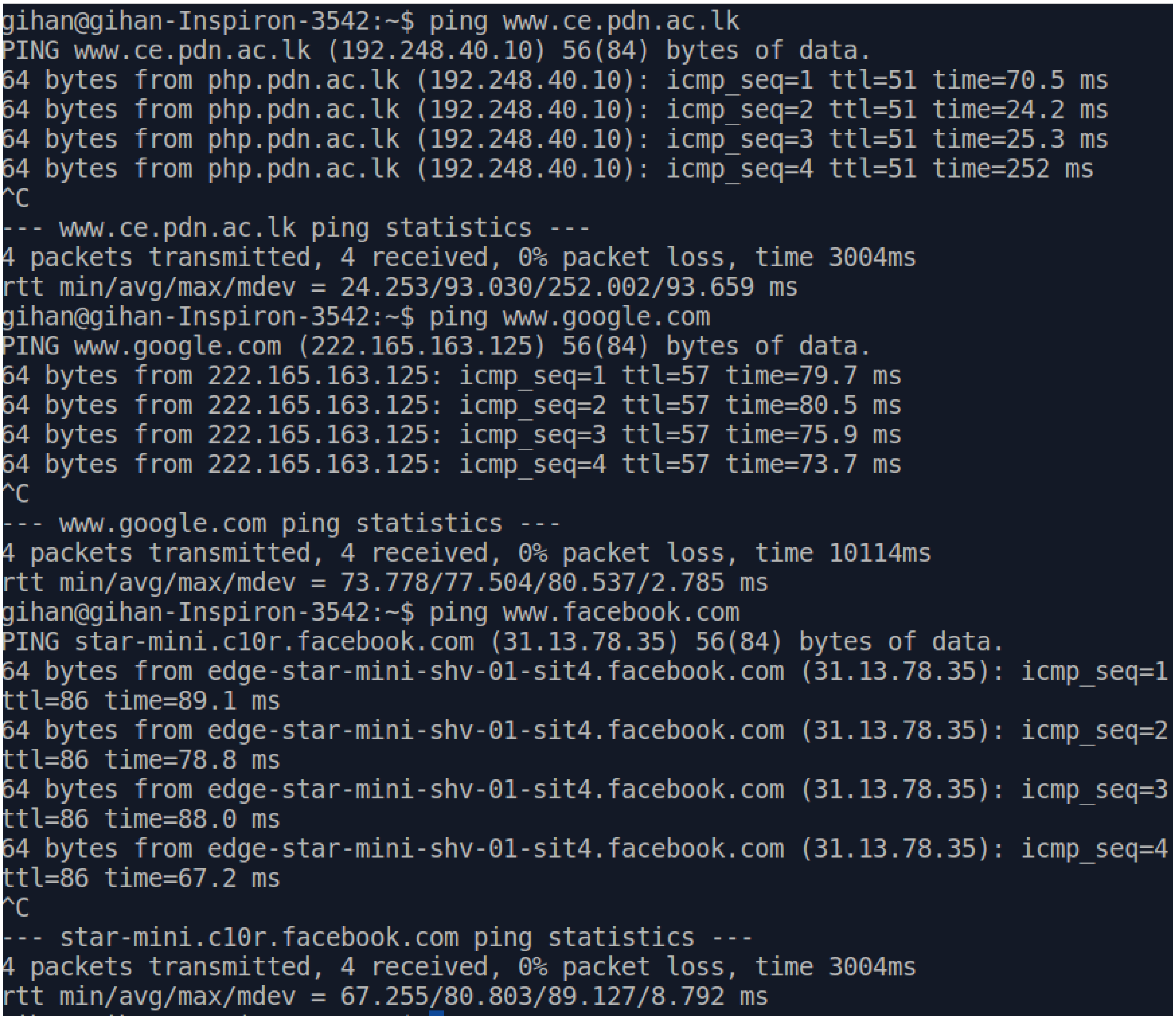
The delay measurement in the network



```
  1     2 ms     2 ms     2 ms  192.168.3.1
  2     2 ms     2 ms     2 ms  192.168.1.2
  3    <1 ms    <1 ms    <1 ms  CENLAB-07 [192.168.4.2]
```

The delay is around 1-2ms for the nodes in the path.

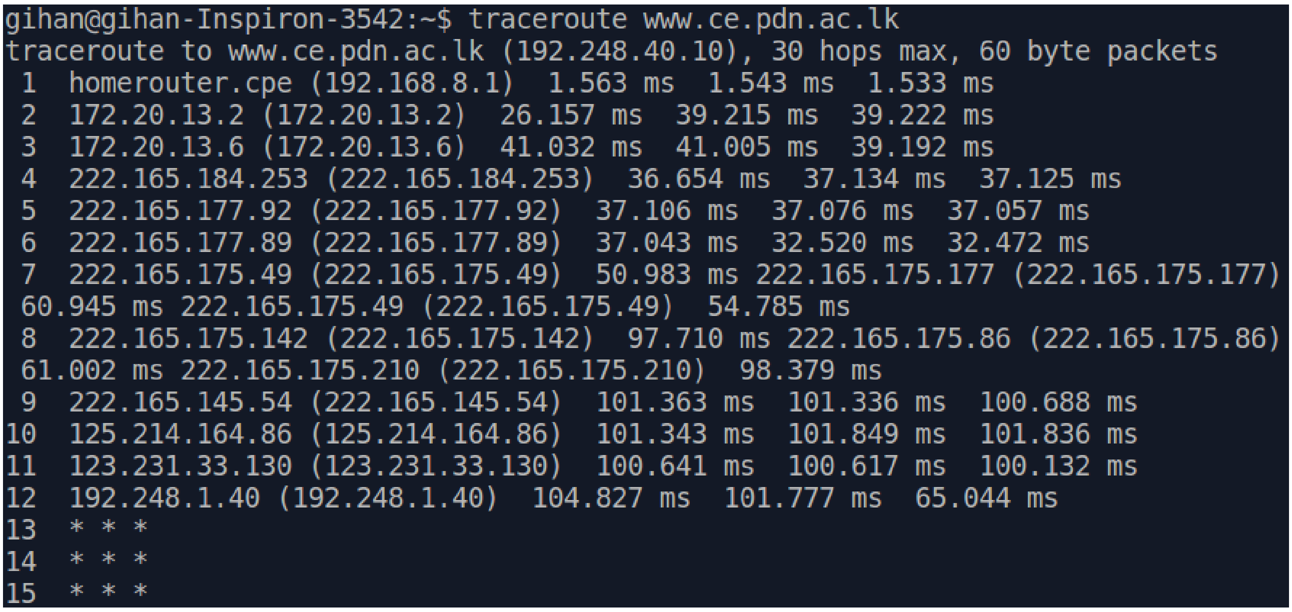
PING ON WEB SITES



```
gihan@gihan-Inspiron-3542:~$ ping www.ce.pdn.ac.lk
PING www.ce.pdn.ac.lk (192.248.40.10) 56(84) bytes of data.
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=1 ttl=51 time=70.5 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=2 ttl=51 time=24.2 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=3 ttl=51 time=25.3 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=4 ttl=51 time=252 ms
^C
--- www.ce.pdn.ac.lk ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 24.253/93.030/252.002/93.659 ms
gihan@gihan-Inspiron-3542:~$ ping www.google.com
PING www.google.com (222.165.163.125) 56(84) bytes of data.
64 bytes from 222.165.163.125: icmp_seq=1 ttl=57 time=79.7 ms
64 bytes from 222.165.163.125: icmp_seq=2 ttl=57 time=80.5 ms
64 bytes from 222.165.163.125: icmp_seq=3 ttl=57 time=75.9 ms
64 bytes from 222.165.163.125: icmp_seq=4 ttl=57 time=73.7 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 10114ms
rtt min/avg/max/mdev = 73.778/77.504/80.537/2.785 ms
gihan@gihan-Inspiron-3542:~$ ping www.facebook.com
PING star-mini.c10r.facebook.com (31.13.78.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-sit4.facebook.com (31.13.78.35): icmp_seq=1
ttl=86 time=89.1 ms
64 bytes from edge-star-mini-shv-01-sit4.facebook.com (31.13.78.35): icmp_seq=2
ttl=86 time=78.8 ms
64 bytes from edge-star-mini-shv-01-sit4.facebook.com (31.13.78.35): icmp_seq=3
ttl=86 time=88.0 ms
64 bytes from edge-star-mini-shv-01-sit4.facebook.com (31.13.78.35): icmp_seq=4
ttl=86 time=67.2 ms
^C
--- star-mini.c10r.facebook.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 67.255/80.803/89.127/8.792 ms
```

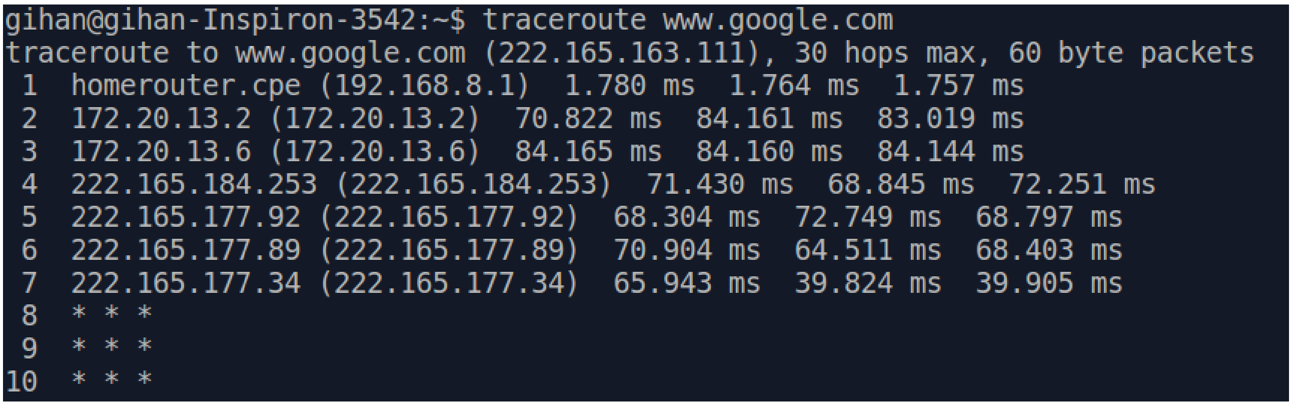
Figure: ping for www.ce.pdn.ac.lk www.google.com www.facebook.com

TRACEROUTE ON WEB SITES



```
gihan@gihan-Inspiron-3542:~$ traceroute www.ce.pdn.ac.lk
traceroute to www.ce.pdn.ac.lk (192.248.40.10), 30 hops max, 60 byte packets
 1  homerouter.cpe (192.168.8.1)  1.563 ms  1.543 ms  1.533 ms
 2  172.20.13.2 (172.20.13.2)  26.157 ms  39.215 ms  39.222 ms
 3  172.20.13.6 (172.20.13.6)  41.032 ms  41.005 ms  39.192 ms
 4  222.165.184.253 (222.165.184.253)  36.654 ms  37.134 ms  37.125 ms
 5  222.165.177.92 (222.165.177.92)  37.106 ms  37.076 ms  37.057 ms
 6  222.165.177.89 (222.165.177.89)  37.043 ms  32.520 ms  32.472 ms
 7  222.165.175.49 (222.165.175.49)  50.983 ms 222.165.175.177 (222.165.175.177)
 60.945 ms 222.165.175.49 (222.165.175.49)  54.785 ms
 8  222.165.175.142 (222.165.175.142)  97.710 ms 222.165.175.86 (222.165.175.86)
 61.002 ms 222.165.175.210 (222.165.175.210)  98.379 ms
 9  222.165.145.54 (222.165.145.54)  101.363 ms  101.336 ms  100.688 ms
10  125.214.164.86 (125.214.164.86)  101.343 ms  101.849 ms  101.836 ms
11  123.231.33.130 (123.231.33.130)  100.641 ms  100.617 ms  100.132 ms
12  192.248.1.40 (192.248.1.40)  104.827 ms  101.777 ms  65.044 ms
13  * * *
14  * * *
15  * * *
```

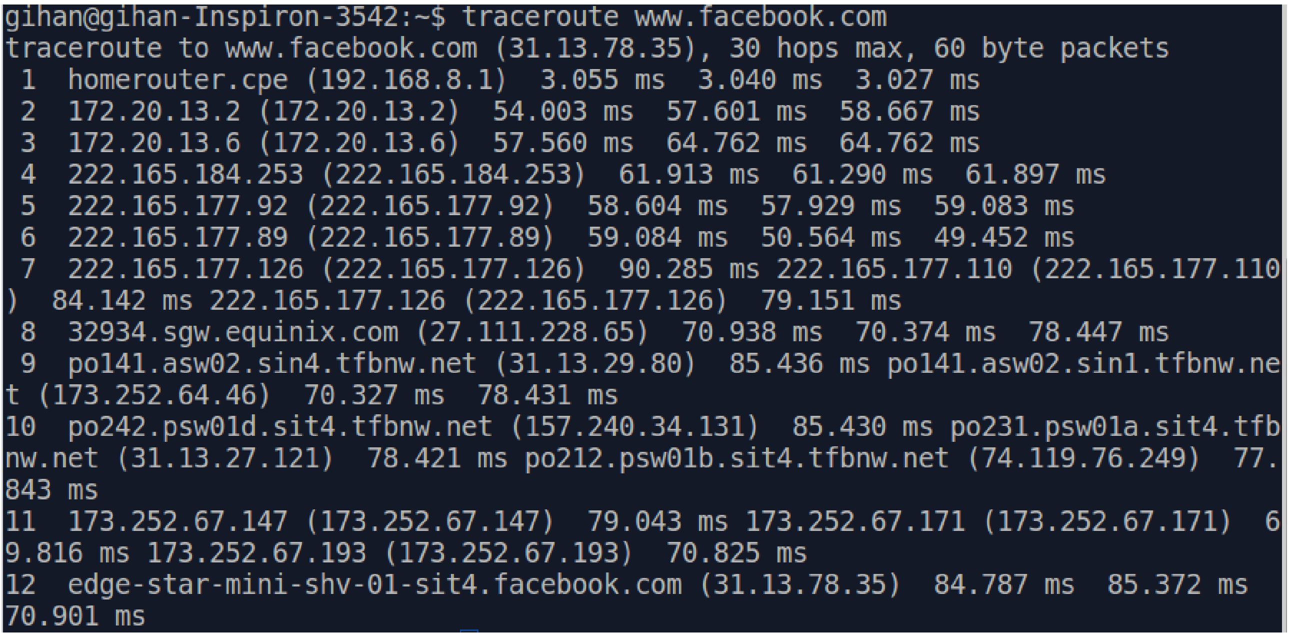
Figure: Traceroute for www.ce.pdn.ac.lk through home router



```
gihan@gihan-Inspiron-3542:~$ traceroute www.google.com
traceroute to www.google.com (222.165.163.111), 30 hops max, 60 byte packets
 1  homerouter.cpe (192.168.8.1)  1.780 ms  1.764 ms  1.757 ms
 2  172.20.13.2 (172.20.13.2)  70.822 ms  84.161 ms  83.019 ms
 3  172.20.13.6 (172.20.13.6)  84.165 ms  84.160 ms  84.144 ms
 4  222.165.184.253 (222.165.184.253)  71.430 ms  68.845 ms  72.251 ms
 5  222.165.177.92 (222.165.177.92)  68.304 ms  72.749 ms  68.797 ms
 6  222.165.177.89 (222.165.177.89)  70.904 ms  64.511 ms  68.403 ms
 7  222.165.177.34 (222.165.177.34)  65.943 ms  39.824 ms  39.905 ms
 8  * * *
 9  * * *
10  * * *
```

Figure: Traceroute for www.google.com through home rout

The traceroute cannot go beyond a certain node in the path when it tries to trace the path to www.ce.pdn.ac.lk and www.google.com most probably because ofa security measure by the servers.



```
gihan@gihan-Inspiron-3542:~$ traceroute www.facebook.com
traceroute to www.facebook.com (31.13.78.35), 30 hops max, 60 byte packets
 1  homerouter.cpe (192.168.8.1)  3.055 ms  3.040 ms  3.027 ms
 2  172.20.13.2 (172.20.13.2)  54.003 ms  57.601 ms  58.667 ms
 3  172.20.13.6 (172.20.13.6)  57.560 ms  64.762 ms  64.762 ms
 4  222.165.184.253 (222.165.184.253)  61.913 ms  61.290 ms  61.897 ms
 5  222.165.177.92 (222.165.177.92)  58.604 ms  57.929 ms  59.083 ms
 6  222.165.177.89 (222.165.177.89)  59.084 ms  50.564 ms  49.452 ms
 7  222.165.177.126 (222.165.177.126)  90.285 ms 222.165.177.110 (222.165.177.110
)  84.142 ms 222.165.177.126 (222.165.177.126)  79.151 ms
 8  32934.sgw.equinix.com (27.111.228.65)  70.938 ms  70.374 ms  78.447 ms
 9  po141.asw02.sin4.tfbnw.net (31.13.29.80)  85.436 ms po141.asw02.sin1.tfbnw.ne
t (173.252.64.46)  70.327 ms  78.431 ms
10  po242.psw01d.sit4.tfbnw.net (157.240.34.131)  85.430 ms po231.psw01a.sit4.tfb
nw.net (31.13.27.121)  78.421 ms po212.psw01b.sit4.tfbnw.net (74.119.76.249)  77.
843 ms
11  173.252.67.147 (173.252.67.147)  79.043 ms 173.252.67.171 (173.252.67.171)  6
9.816 ms 173.252.67.193 (173.252.67.193)  70.825 ms
12  edge-star-mini-shv-01-sit4.facebook.com (31.13.78.35)  84.787 ms  85.372 ms
70.901 ms
```

Figure: Traceroute for www.facebook.com through home router

The delay does not strictly increase for every node from the source. It is because of,

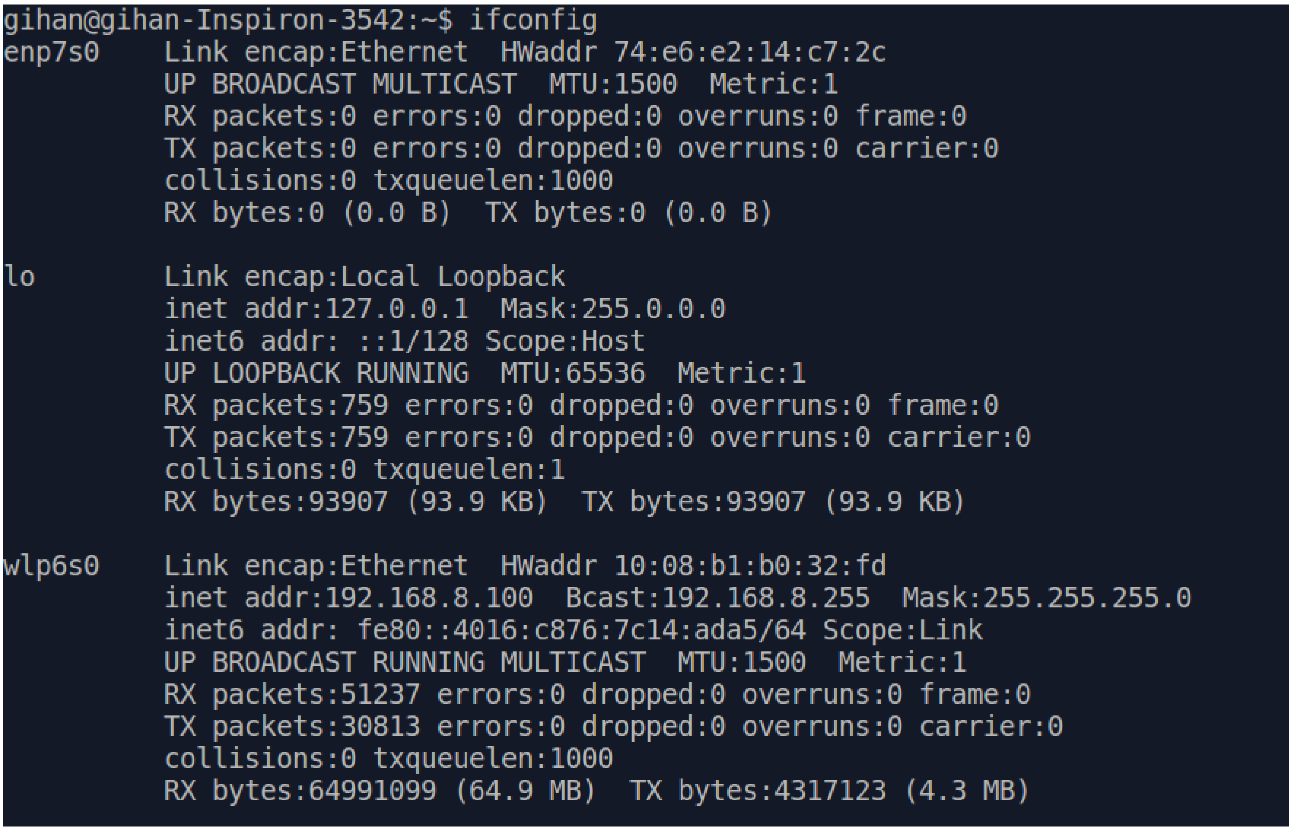
1. The delay from a node in the path depends on two factors-- the speed that the routers in the path can forward traffic and the speed the end node can respond to ping. Suppose that a router close to the source has high delay in responding to the ping but can transfer traffic faster, the next router which has a fast ping response can get a lower delay than the previous one.

2.Even though the later nodes in the path have more hops from the source in the path we consider for the trace route, the path the packets take in the return journey may be shorter in the number of hops.

NETWORK TOOLS AND COMMANDS

ifconfig

A tool used to configure network interfaces. Displays the ip addresses and the mac addresses.



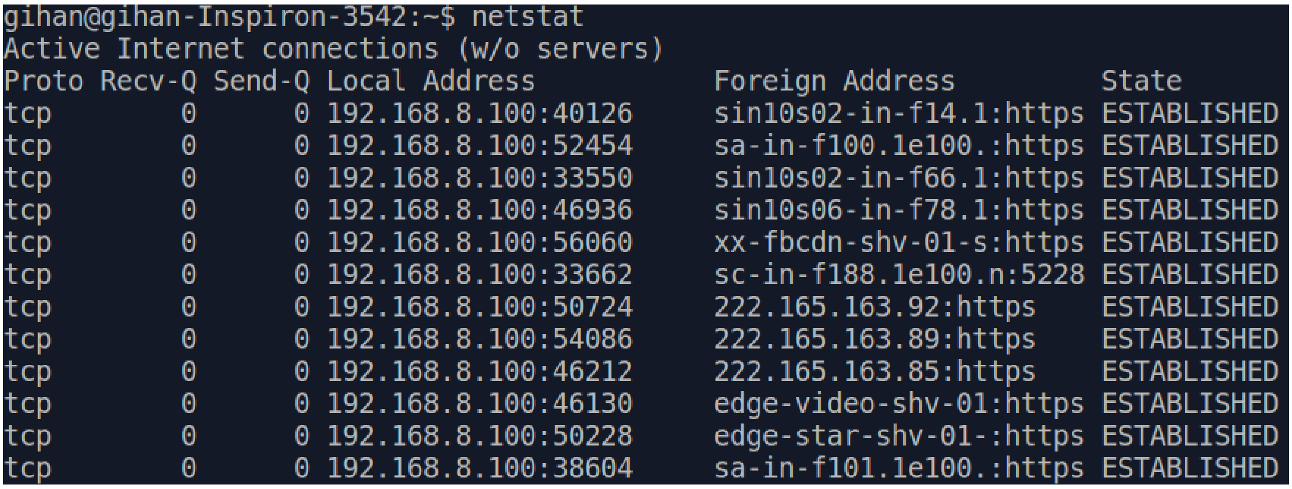
```
gihan@gihan-Inspiron-3542:~$ ifconfig
enp7s0    Link encap:Ethernet  HWaddr 74:e6:e2:14:c7:2c
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:759 errors:0 dropped:0 overruns:0 frame:0
          TX packets:759 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:93907 (93.9 KB)  TX bytes:93907 (93.9 KB)

wlp6s0    Link encap:Ethernet  HWaddr 10:08:b1:b0:32:fd
          inet addr:192.168.8.100  Bcast:192.168.8.255  Mask:255.255.255.0
          inet6 addr: fe80::4016:c876:7c14:ada5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:51237 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30813 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:64991099 (64.9 MB)  TX bytes:4317123 (4.3 MB)
```

Netstat

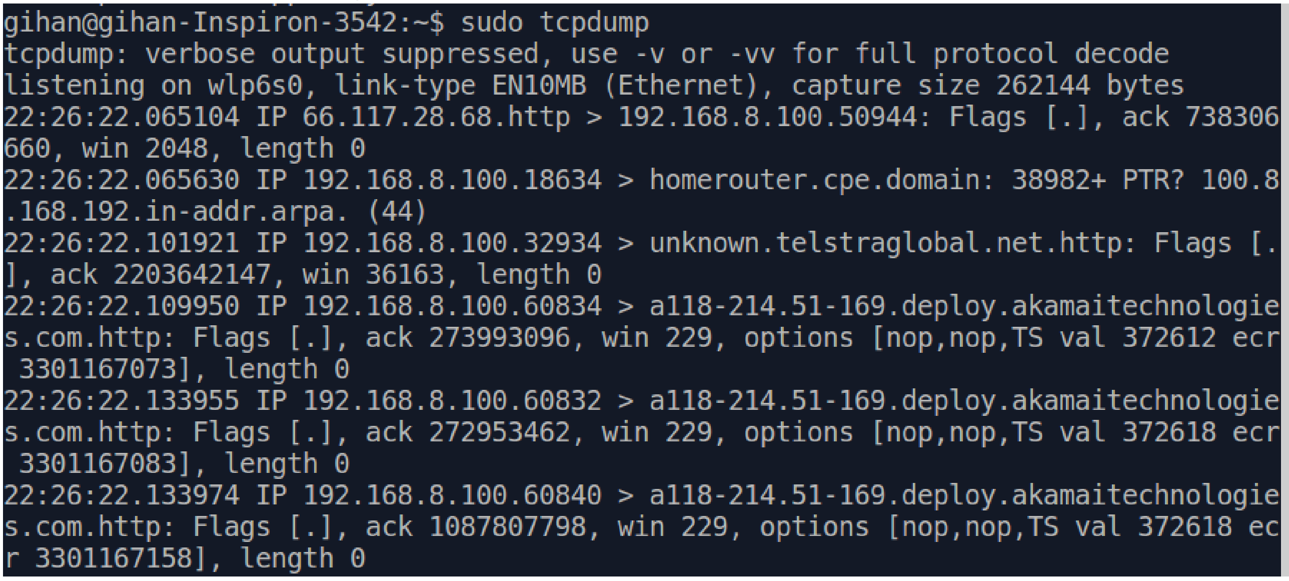
A command line tool that display all the information regarding the network connections of a computer. (Only a part of the information displayed is in the screen shot below.)



```
gihan@gihan-Inspiron-3542:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.8.100:40126     sin10s02-in-f14.1:https ESTABLISHED
tcp        0      0 192.168.8.100:52454     sa-in-f100.1e100.:https ESTABLISHED
tcp        0      0 192.168.8.100:33550     sin10s02-in-f66.1:https ESTABLISHED
tcp        0      0 192.168.8.100:46936     sin10s06-in-f78.1:https ESTABLISHED
tcp        0      0 192.168.8.100:56060     xx-fbcdn-shv-01-s:https ESTABLISHED
tcp        0      0 192.168.8.100:33662     sc-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 192.168.8.100:50724     222.165.163.92:https    ESTABLISHED
tcp        0      0 192.168.8.100:54086     222.165.163.89:https    ESTABLISHED
tcp        0      0 192.168.8.100:46212     222.165.163.85:https    ESTABLISHED
tcp        0      0 192.168.8.100:46130     edge-video-shv-01:https ESTABLISHED
tcp        0      0 192.168.8.100:50228     edge-star-shv-01-:https ESTABLISHED
tcp        0      0 192.168.8.100:38604     sa-in-f101.1e100.:https ESTABLISHED
```

Tcpdump

This is a packet analyzer.



```
gihan@gihan-Inspiron-3542:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp6s0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:26:22.065104 IP 66.117.28.68.http > 192.168.8.100.50944: Flags [.], ack 738306
660, win 2048, length 0
22:26:22.065630 IP 192.168.8.100.18634 > homerouter.cpe.domain: 38982+ PTR? 100.8
.168.192.in-addr.arpa. (44)
22:26:22.101921 IP 192.168.8.100.32934 > unknown.telstraglobal.net.http: Flags [.
], ack 2203642147, win 36163, length 0
22:26:22.109950 IP 192.168.8.100.60834 > a118-214.51-169.deploy.akamaitechnologie
s.com.http: Flags [.], ack 273993096, win 229, options [nop,nop,TS val 372612 ecr
 3301167073], length 0
22:26:22.133955 IP 192.168.8.100.60832 > a118-214.51-169.deploy.akamaitechnologie
s.com.http: Flags [.], ack 272953462, win 229, options [nop,nop,TS val 372618 ecr
 3301167083], length 0
22:26:22.133974 IP 192.168.8.100.60840 > a118-214.51-169.deploy.akamaitechnologie
s.com.http: Flags [.], ack 1087807798, win 229, options [nop,nop,TS val 372618 ec
r 3301167158], length 0
```

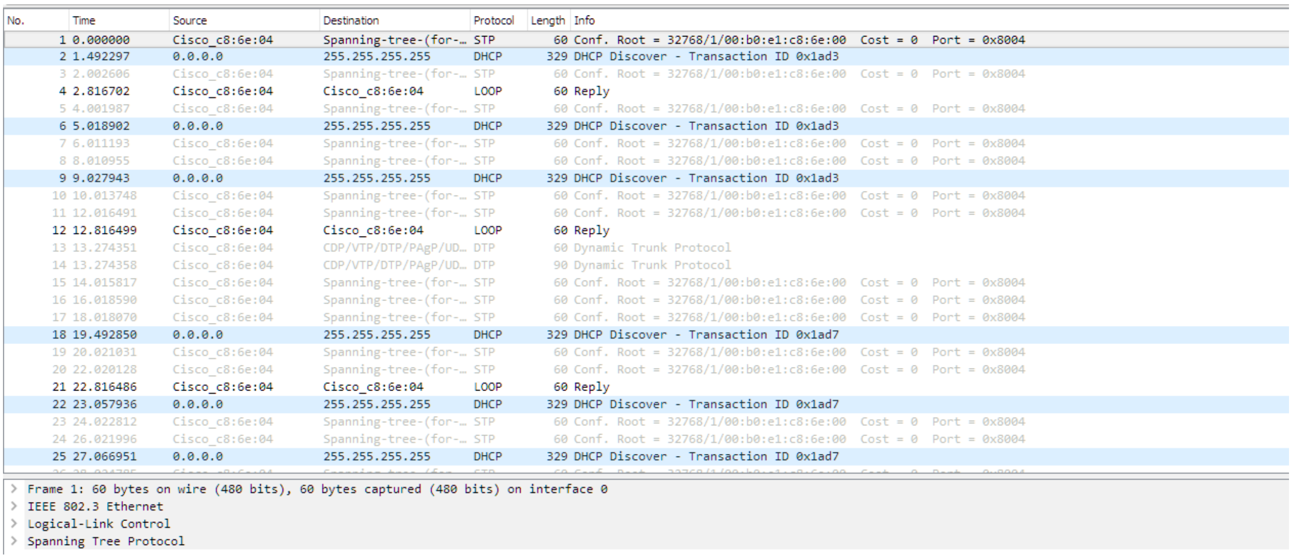
NETWORK PROTOCOL ANALYZER

What is a network protocol analyzer?

This is a tool used to monitor the data (packets, signals etc) on a network. This could be a sophisticated hardware software system or else just a software running on generic PC network infrastructure.

Network analyzers are a must when it comes to maintaining servers, complex networks etc; The anti virus programs have inbuilt network analyzers to spot the threats.

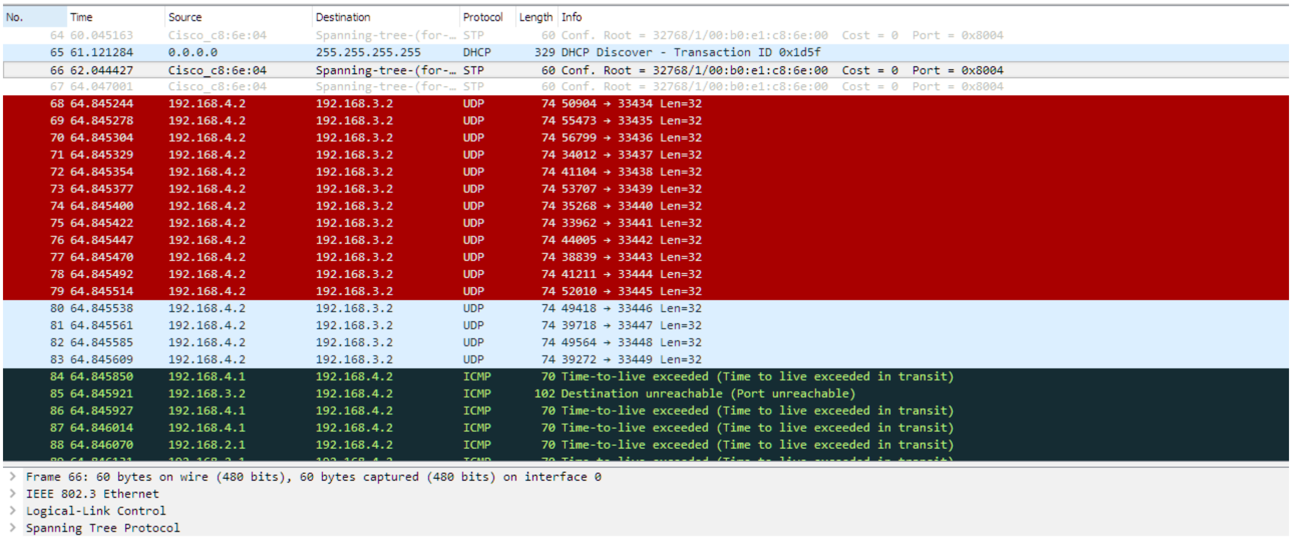
Network traffic during quiet time



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
2	1.492297	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transaction ID 0x1ad3
3	2.002606	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
4	2.816702	Cisco_c8:6e:04	Cisco_c8:6e:04	LOOP	60	Reply
5	4.001987	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
6	5.018902	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transaction ID 0x1ad3
7	6.011193	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
8	8.010955	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
9	9.027943	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transaction ID 0x1ad3
10	10.013748	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
11	12.016491	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
12	12.816499	Cisco_c8:6e:04	Cisco_c8:6e:04	LOOP	60	Reply
13	13.274351	Cisco_c8:6e:04	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
14	13.274358	Cisco_c8:6e:04	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
15	14.015817	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
16	16.018590	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
17	18.018070	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
18	19.492850	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transaction ID 0x1ad7
19	20.021031	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
20	22.020128	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
21	22.816486	Cisco_c8:6e:04	Cisco_c8:6e:04	LOOP	60	Reply
22	23.057936	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transaction ID 0x1ad7
23	24.022812	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
24	26.021996	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
25	27.066951	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transaction ID 0x1ad7

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
> Spanning Tree Protocol
```

Network traffic during busy time



No.	Time	Source	Destination	Protocol	Length	Info
64	60.045163	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
65	61.121284	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transaction ID 0x1d5f
66	62.044427	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
67	64.047001	Cisco_c8:6e:04	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:b0:e1:c8:6e:00 Cost = 0 Port = 0x8004
68	64.845244	192.168.4.2	192.168.3.2	UDP	74	50904 → 33434 Len=32
69	64.845278	192.168.4.2	192.168.3.2	UDP	74	55473 → 33435 Len=32
70	64.845304	192.168.4.2	192.168.3.2	UDP	74	56799 → 33436 Len=32
71	64.845329	192.168.4.2	192.168.3.2	UDP	74	34012 → 33437 Len=32
72	64.845354	192.168.4.2	192.168.3.2	UDP	74	41104 → 33438 Len=32
73	64.845377	192.168.4.2	192.168.3.2	UDP	74	53707 → 33439 Len=32
74	64.845400	192.168.4.2	192.168.3.2	UDP	74	35268 → 33440 Len=32
75	64.845422	192.168.4.2	192.168.3.2	UDP	74	33962 → 33441 Len=32
76	64.845447	192.168.4.2	192.168.3.2	UDP	74	44005 → 33442 Len=32
77	64.845470	192.168.4.2	192.168.3.2	UDP	74	38839 → 33443 Len=32
78	64.845492	192.168.4.2	192.168.3.2	UDP	74	41211 → 33444 Len=32
79	64.845514	192.168.4.2	192.168.3.2	UDP	74	52010 → 33445 Len=32
80	64.845538	192.168.4.2	192.168.3.2	UDP	74	49418 → 33446 Len=32
81	64.845561	192.168.4.2	192.168.3.2	UDP	74	39718 → 33447 Len=32
82	64.845585	192.168.4.2	192.168.3.2	UDP	74	49564 → 33448 Len=32
83	64.845609	192.168.4.2	192.168.3.2	UDP	74	39272 → 33449 Len=32
84	64.845850	192.168.4.1	192.168.4.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	64.845921	192.168.3.2	192.168.4.2	ICMP	102	Destination unreachable (Port unreachable)
86	64.845927	192.168.4.1	192.168.4.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
87	64.846014	192.168.4.1	192.168.4.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
88	64.846070	192.168.2.1	192.168.4.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	64.846131	192.168.2.1	192.168.4.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```
> Frame 66: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
> Spanning Tree Protocol
```

Differences between quiet and busy network traffic

In the quiet network the packets are from various protocols and they have different destination ips. It looks random. The protocols are DHPC, STP etc.

When the network becomes busy, the packets from UDP and ICMP protocols start appearing in large amounts. Most of the packets have the same destination. And also the rate at which the packets appear increases.