

Computer Networks Lab - Week 1

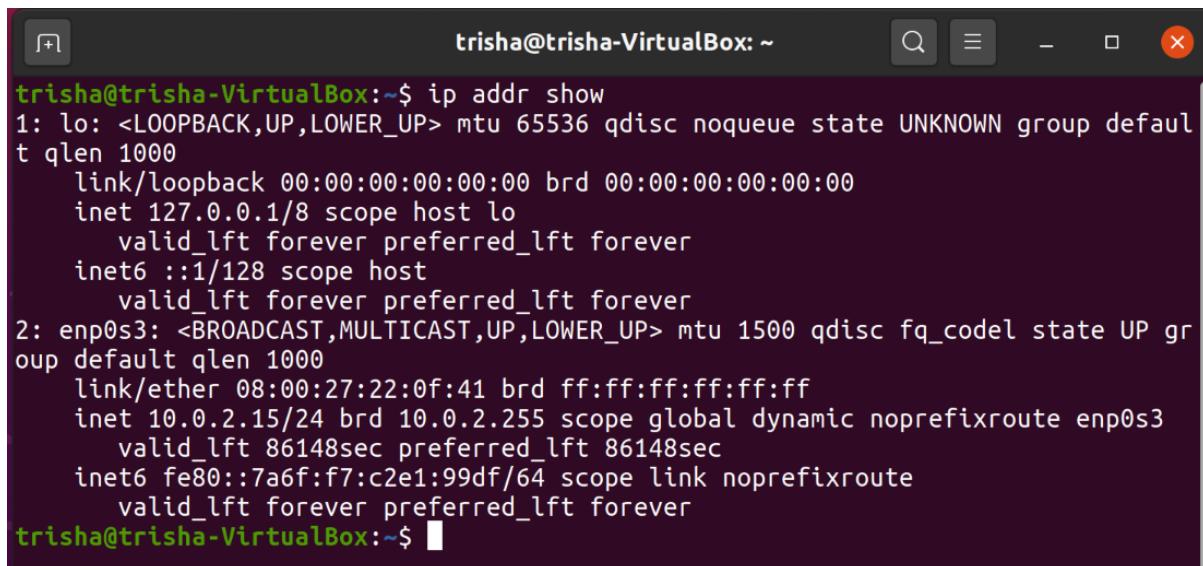
SRN : PES1UG19CS542

Name : Trisha Jain

Task 1: Linux Interface Configuration (ifconfig / IP command)

Step 1: To display status of all active network interfaces.

`ip addr show`

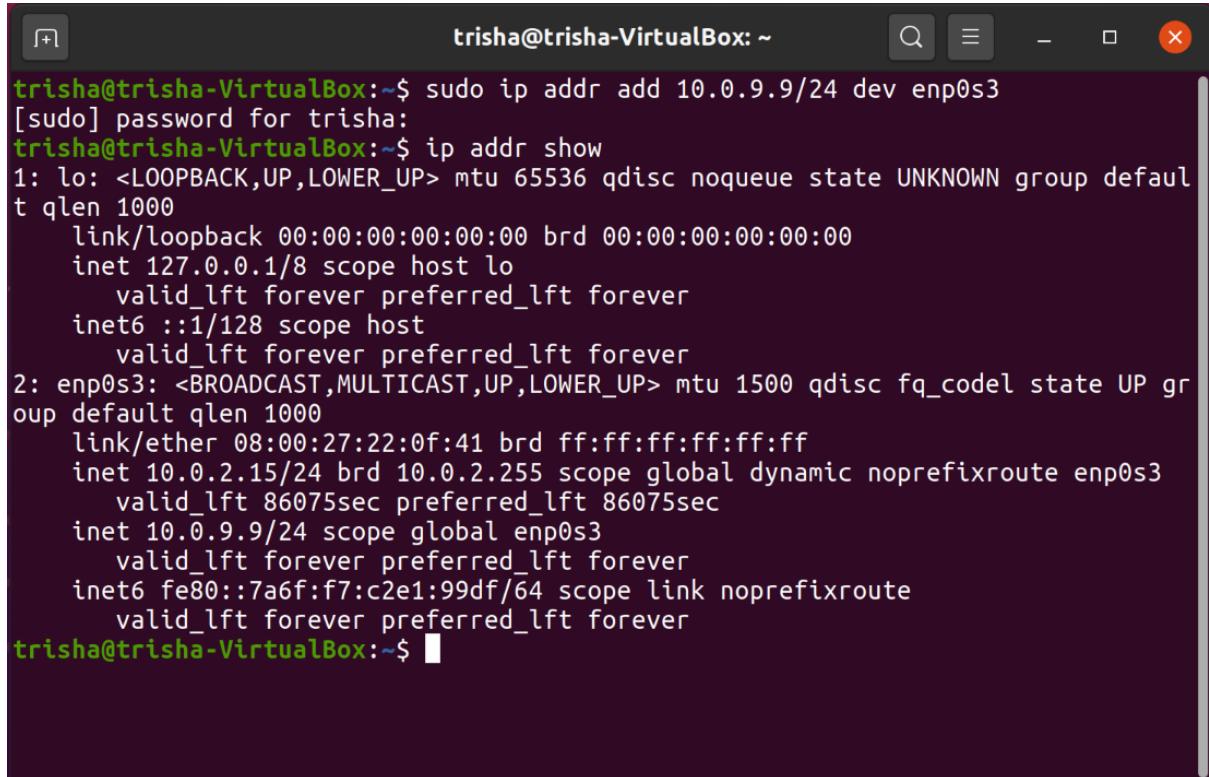


```
trisha@trisha-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:0f:41 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86148sec preferred_lft 86148sec
        inet6 fe80::7a6f:f7:c2e1:99df/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
trisha@trisha-VirtualBox:~$
```

Interface Name	IP Address(IPv4 / IPv6)	MAC Address
lo	127.0.0.1 / ::1	00:00:00:00:00:00
enp0s3	10.0.2.15 / fe80::7a6f:f7:c2e1:99df	08:00:27:22:0f:41

Step 2 : To assign an IP address to an interface, used the following command:

`sudo ip addr add 10.0.9.9 /24 dev enp0s3`



```
trisha@trisha-VirtualBox:~$ sudo ip addr add 10.0.9.9/24 dev enp0s3
[sudo] password for trisha:
trisha@trisha-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:0f:41 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86075sec preferred_lft 86075sec
    inet 10.0.9.9/24 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::7a6f:f7:c2e1:99df/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
trisha@trisha-VirtualBox:~$
```

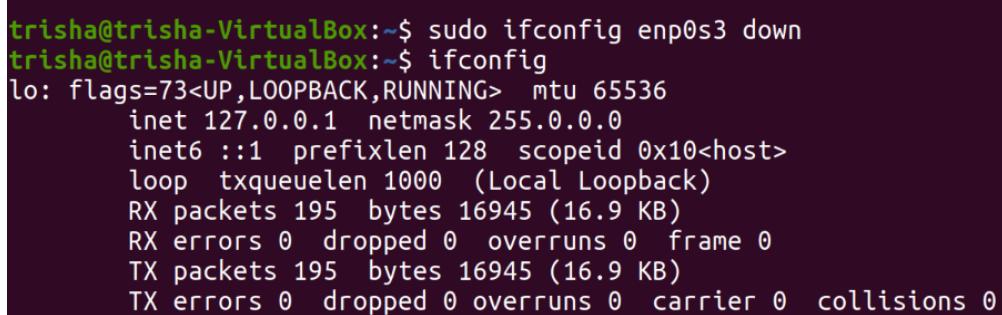
inet 10.0.9.9/24 scope global enp0s3

Step 3 : To activate and deactivate a network interface :

To Deactivate :

Command used is:-

`sudo ifconfig enp0s3 down`



```
trisha@trisha-VirtualBox:~$ sudo ifconfig enp0s3 down
trisha@trisha-VirtualBox:~$ 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 195 bytes 16945 (16.9 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 195 bytes 16945 (16.9 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Only lo is displayed above

To Activate :

Command used is:-

`sudo ifconfig enp0s3 up`

```
trisha@trisha-VirtualBox:~$ sudo ifconfig enp0s3 up
trisha@trisha-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::7a6f:f7:c2e1:99df prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:22:0f:41 txqueuelen 1000 (Ethernet)
            RX packets 4329 bytes 5679155 (5.6 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 2463 bytes 169851 (169.8 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 217 bytes 18635 (18.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 217 bytes 18635 (18.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

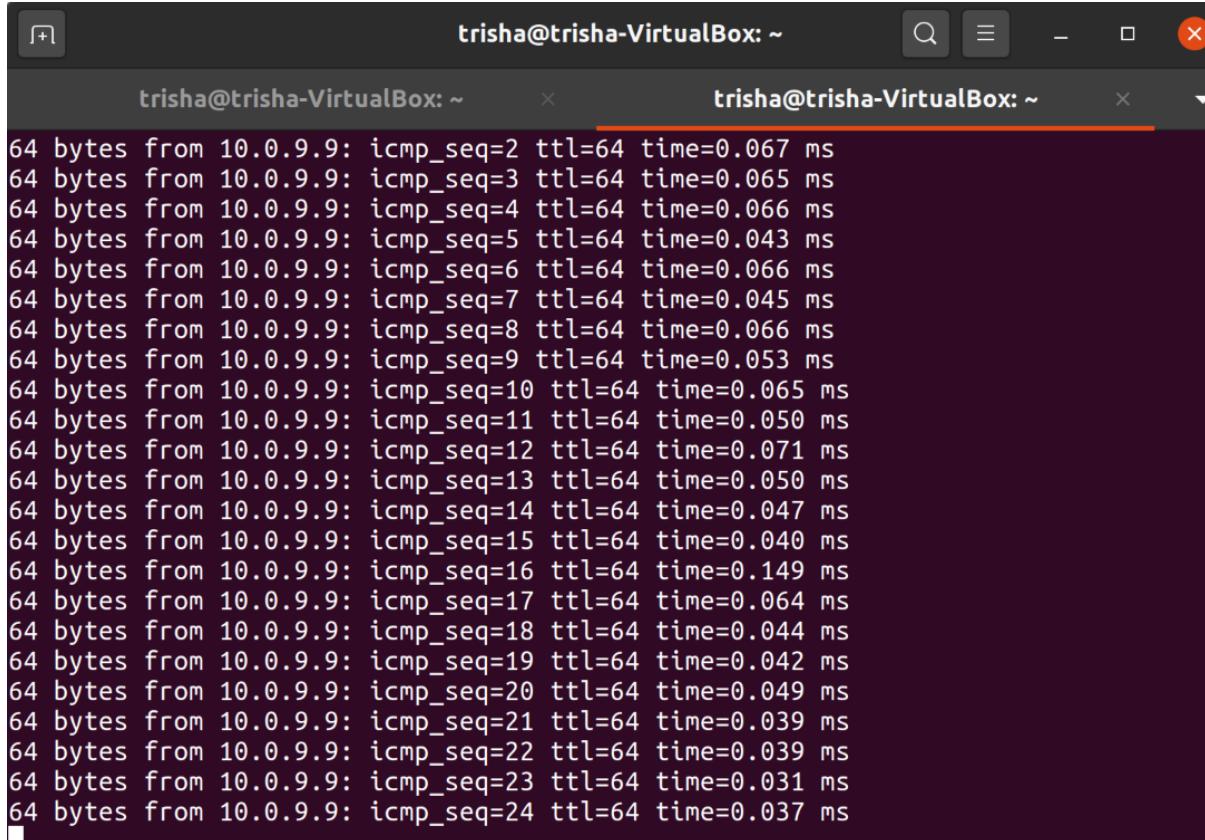
trisha@trisha-VirtualBox:~$ █
```

Now enp0s3 is also shown since its reactivated

Step 4 : To show the current neighbour table in kernel, ip neigh is used.

```
trisha@trisha-VirtualBox:~$ ip neigh
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
      ip neigh
```

Task 2: Ping PDU (Packet Data Units or Packets) Capture



The screenshot shows a terminal window with two tabs, both titled "trisha@trisha-VirtualBox: ~". The terminal is displaying the output of a ping command to the IP address 10.0.9.9. The output consists of 24 lines, each representing a ICMP echo request (ping) sent to 10.0.9.9. The lines show the sequence number (icmp_seq), TTL (ttl), and time taken for each response. The responses are timestamped from 0.031 ms to 0.067 ms.

```
64 bytes from 10.0.9.9: icmp_seq=2 ttl=64 time=0.067 ms
64 bytes from 10.0.9.9: icmp_seq=3 ttl=64 time=0.065 ms
64 bytes from 10.0.9.9: icmp_seq=4 ttl=64 time=0.066 ms
64 bytes from 10.0.9.9: icmp_seq=5 ttl=64 time=0.043 ms
64 bytes from 10.0.9.9: icmp_seq=6 ttl=64 time=0.066 ms
64 bytes from 10.0.9.9: icmp_seq=7 ttl=64 time=0.045 ms
64 bytes from 10.0.9.9: icmp_seq=8 ttl=64 time=0.066 ms
64 bytes from 10.0.9.9: icmp_seq=9 ttl=64 time=0.053 ms
64 bytes from 10.0.9.9: icmp_seq=10 ttl=64 time=0.065 ms
64 bytes from 10.0.9.9: icmp_seq=11 ttl=64 time=0.050 ms
64 bytes from 10.0.9.9: icmp_seq=12 ttl=64 time=0.071 ms
64 bytes from 10.0.9.9: icmp_seq=13 ttl=64 time=0.050 ms
64 bytes from 10.0.9.9: icmp_seq=14 ttl=64 time=0.047 ms
64 bytes from 10.0.9.9: icmp_seq=15 ttl=64 time=0.040 ms
64 bytes from 10.0.9.9: icmp_seq=16 ttl=64 time=0.149 ms
64 bytes from 10.0.9.9: icmp_seq=17 ttl=64 time=0.064 ms
64 bytes from 10.0.9.9: icmp_seq=18 ttl=64 time=0.044 ms
64 bytes from 10.0.9.9: icmp_seq=19 ttl=64 time=0.042 ms
64 bytes from 10.0.9.9: icmp_seq=20 ttl=64 time=0.049 ms
64 bytes from 10.0.9.9: icmp_seq=21 ttl=64 time=0.039 ms
64 bytes from 10.0.9.9: icmp_seq=22 ttl=64 time=0.039 ms
64 bytes from 10.0.9.9: icmp_seq=23 ttl=64 time=0.031 ms
64 bytes from 10.0.9.9: icmp_seq=24 ttl=64 time=0.037 ms
```

ping 10.0.9.9

TTL	64
Protocol used by ping	ICMP
Time	Order of 10^{-2} ms

No.	Time	Source	Destination	Protocol	Length	Info
10	10.000000000	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in)
10	20.000007315	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in)
31	029659867	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in)
41	029677294	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in)
52	053457736	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in)
62	053474017	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in)
73	077469199	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in)
83	077486387	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in)
94	101531062	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in)
104	101541743	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in)
115	125296180	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in)
125	125312856	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request in)
136	149561912	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in)

Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0

- > Interface id: 0 (any)
 - Encapsulation type: Linux cooked-mode capture v1 (25)
 - Arrival Time: Jan 19, 2021 17:47:22.423184414 IST
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1611058642.423184414 seconds
 - [Time delta from previous captured frame: 0.000000000 seconds]
 - [Time delta from previous displayed frame: 0.000000000 seconds]
 - [Time since reference or first frame: 0.000000000 seconds]
 - Frame Number: 1
 - Frame Length: 100 bytes (800 bits)
 - Capture Length: 100 bytes (800 bits)
 - [Frame is marked: False]
 - [Frame is ignored: False]
 - [Protocols in frame: sll:ethertype:ip:icmp:data]
 - [Coloring Rule Name: ICMP]
 - [Coloring Rule String: icmp || icmpv6]
- > Linux cooked capture v1
 - Packet type: Unicast to us (0)
 - Link-layer address type: Loopback (772)
 - Link-layer address length: 6
 - Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
 - Unused: 0000
 - Protocol: IPv4 (0x0800)
- > Internet Protocol Version 4, Src: 10.0.9.9, Dst: 10.0.9.9
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0xe088 (57480)
 - > Flags: 0x40, Don't fragment
 - Fragment Offset: 0
 - Time to Live: 64
 - Protocol: ICMP (1)
 - Header Checksum: 0x340f [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 10.0.9.9
 - Destination Address: 10.0.9.9
- > Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x5888 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 1 (0x0001)
 - Sequence Number (LE): 256 (0x0100)
 - [Response frame: 2]
 - Timestamp from icmp data: Jan 19, 2021 17:47:22.000000000 IST
 - [Timestamp from icmp data (relative): 0.423184414 seconds]
 - > Data (48 bytes)

Request Packet

No.	Time	Source	Destination	Protocol	Length	Info
1	10.0000000000	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in)
2	0.000007315	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request)
3	1.029659867	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in)
4	1.029677294	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request)
5	2.053457736	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in)
6	2.053474017	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request)
7	3.077469199	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in)
8	3.077486387	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request)
9	4.101531862	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in)
10	4.101541743	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request)
11	5.125296180	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in)
12	5.125312856	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request)
13	6.149561912	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in)
14	6.149572100	10.0.9.9	10.0.9.9	ICMP	100	Echo (ping) reply id=0x0001, seq=7/1792, ttl=64 (request)
Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0						
Interface id: 0 (any) Encapsulation type: Linux cooked-mode capture v1 (25) Arrival Time: Jan 19, 2021 17:47:22.423191729 IST [Time shift for this packet: 0.00000000 seconds] Epoch Time: 1611058642.423191729 seconds [Time delta from previous captured frame: 0.000007315 seconds] [Time delta from previous displayed frame: 0.000007315 seconds] [Time since reference or first frame: 0.000007315 seconds] Frame Number: 2 Frame Length: 100 bytes (800 bits) Capture Length: 100 bytes (800 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: sll:ethertype:ip:icmp:data] [Coloring Rule Name: ICMP] [Coloring Rule String: icmp icmpv6]						
Linux cooked capture v1 Packet type: Unicast to us (0) Link-layer address type: Loopback (772) Link-layer address length: 6 Source: 00:00:00_00:00:00 (00:00:00:00:00:00) Unused: 0000 Protocol: IPv4 (0x0800)						
Internet Protocol Version 4, Src: 10.0.9.9, Dst: 10.0.9.9 0100 . . . = Version: 4 . .0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 84 Identification: 0xe089 (57481) Flags: 0x00 Fragment Offset: 0 Time to Live: 64 Protocol: ICMP (1) Header Checksum: 0x740e [validation disabled] [Header checksum status: Unverified] Source Address: 10.0.9.9 Destination Address: 10.0.9.9						
Internet Control Message Protocol Type: 0 (Echo (ping) reply) Code: 0 Checksum: 0x6088 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence Number (BE): 1 (0x0001) Sequence Number (LE): 256 (0x0100) [Request frame: 1] [Response time: 0.007 ms] Timestamp from icmp data: Jan 19, 2021 17:47:22.000000000 IST [Timestamp from icmp data (relative): 0.423191729 seconds]						
> Data (48 bytes)						

Response Packet

Details	First Echo Request	First Echo Reply
Frame Number	1	2
Source IP Address	10.0.9.9	10.0.9.9
Destination IP Address	10.0.9.9	10.0.9.9
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	IPv4	IPv4
TTL Value	64	64

Task 3: HTTP PDU (Packet Data Units or Packets) Capture

```
> Frame 3373: 391 bytes on wire (3128 bits), 391 bytes captured (3128 bits) on interface any, id 0
  Linux cooked capture v1
    Packet type: Sent by us (4)
    Link-layer address type: Ethernet (1)
    Link-layer address length: 6
    Source: PcsCompu_22:0F:41 (08:00:27:22:0F:41)
    Unused: 5341
    Protocol: IPv4 (0x0800)
-> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 163.53.78.110
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 375
  Identification: 0xf3f7 (62455)
  Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x47d7 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 163.53.78.110
-> Transmission Control Protocol, Src Port: 33420, Dst Port: 80, Seq: 1, Ack: 1, Len: 335
  Source Port: 33420
  Destination Port: 80
  [Stream index: 30]
  [TCP Segment Len: 335]
  Sequence Number: 1      (relative sequence number)
  Sequence Number (raw): 1988145383
  [Next Sequence Number: 336      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 28864002
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 64240
  [Calculated window size: 64240]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0xfffb [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
  TCP payload (335 bytes)
-> Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
  Host: www.flipkart.com\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://www.flipkart.com/]
  [HTTP request 1/1]
  [Response in frame: 3563]
```

Request Packet

```

> Frame 3563: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface any, id 0
  ▾ Linux cooked capture v1
    Packet type: Unicast to us (0)
    Link-layer address type: Ethernet (1)
    Link-layer address length: 6
    Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Unused: 0302
    Protocol: IPv4 (0x0800)
  ▾ Internet Protocol Version 4, Src: 163.53.78.110, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 411
    Identification: 0x80b9 (32953)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xfaf1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 163.53.78.110
    Destination Address: 10.0.2.15
  ▾ Transmission Control Protocol, Src Port: 80, Dst Port: 33420, Seq: 1, Ack: 336, Len: 371
    Source Port: 80
    Destination Port: 33420
    [Stream index: 30]
    [TCP Segment Len: 371]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 28864002
    [Next Sequence Number: 372 (relative sequence number)]
    Acknowledgment Number: 336 (relative ack number)
    Acknowledgment number (raw): 1988145718
    0101 .... = Header Length: 20 bytes (5)
    ▾ Flags: 0x018 (PSH, ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xabad [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    ▾ [SEQ/ACK analysis]
    ▾ [Timestamps]
    ▾ TCP payload (371 bytes)
  ▾ Hypertext Transfer Protocol
    ▾ HTTP/1.1 301 Moved Permanently\r\n
      Server: nginx\r\n
      Date: Tue, 19 Jan 2021 12:31:56 GMT\r\n
      Content-Type: text/html\r\n
      Location: https://www.flipkart.com/\r\n
      Content-Length: 178\r\n
      Connection: keep-alive\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 1.558474068 seconds]
      [Request in frame: 3373]
      [Request URI: http://www.flipkart.com/]
      File Data: 178 bytes
  ▾ Line-based text data: text/html (7 lines)

```

Response Packet

Details	First Echo Request	First Echo Reply
Frame Number	3373	3563
Source Port	33420	80
Destination Port	80	33420
Source IP Address	10.0.2.15	163.53.78.110
Destination IP Address	163.53.78.110	10.0.2.15
Source Ethernet Address	08:00:27:22:0f:41	52:54:00:12:35:02
Destination Ethernet Address	52:54:00:12:35:02	08:00:27:22:0f:41

HTTP Request and Response

HTTP Request		HTTP Response	
Get	GET/HTTP/1.1\r\n	Server	nginx
Host	www.flipkart.com	Content-Type	text/html
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/80.0	Date	Tue, 19 Jan 2021 12:31:56 GMT
Accept-Language	en-US,en;q=0.5	Location	https://www.flipkart.com/
Accept-Encoding	gzip, deflate	Content-Length	178
Connection	keep-alive	Connection	keep-alive

Using Wireshark to follow TCP Stream

The screenshot shows the Wireshark interface with a single TCP stream selected. The title bar reads "Wireshark · Follow TCP Stream (tcp.stream eq 30) · any". The main pane displays the raw HTTP exchange:

```
GET / HTTP/1.1
Host: www.flipkart.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Tue, 19 Jan 2021 12:31:56 GMT
Content-Type: text/html
Location: https://www.flipkart.com/
Content-Length: 178
Connection: keep-alive

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

At the bottom of the main pane, it says "1 client pkt, 1 server pkt, 1 turn.". Below the pane are several control buttons and dropdowns:

- Entire conversation (706 bytes)
- Show data as ASCII
- Stream 30
- Find: Find Next
- Help
- Filter Out This Stream
- Print
- Save as...
- Back
- Close

Task 4: Capturing Packets with tcpdump

Step 1: Using the command `sudo tcpdump -D` to see which interfaces are available for capture.

```
trisha@trisha-VirtualBox:~$ sudo tcpdump -D
[sudo] password for trisha:
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
trisha@trisha-VirtualBox:~$
```

`sudo tcpdump -D`

Step 2: Using the command `sudo tcpdump -i any` to capture all packets in any interface.

```
trisha@trisha-VirtualBox:~$ sudo tcpdump -i any
18:22:46.796509 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo request, id 2, seq 27, length 64
18:22:46.796529 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo reply, id 2, seq 27, length 64
18:22:47.820780 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo request, id 2, seq 28, length 64
18:22:47.820792 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo reply, id 2, seq 28, length 64
18:22:48.844621 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo request, id 2, seq 29, length 64
18:22:48.844641 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo reply, id 2, seq 29, length 64
18:22:49.036419 IP trisha-VirtualBox.47396 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 244, win 63996, length 0
18:22:49.036477 IP trisha-VirtualBox.60412 > maa03s29-in-f14.1e100.net.http: Flags [.], ack 553, win 64032, length 0
18:22:49.037037 IP 82.221.107.34.bc.googleusercontent.com.http > trisha-VirtualBox.47396: Flags [.], ack 1, win 65535, length 0
18:22:49.037038 IP maa03s29-in-f14.1e100.net.http > trisha-VirtualBox.60412: Flags [.], ack 330, win 65535, length 0
18:22:49.292298 IP trisha-VirtualBox.47398 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 245, win 63996, length 0
18:22:49.292380 IP trisha-VirtualBox.34928 > maa03s28-in-f4.1e100.net.http: Flags [.], ack 633, win 63832, length 0
```

`sudo tcpdump -i any`

Step 3: Understanding the output format of tcpdump :-

Using the following line as an example :-

```
18:22:49.292298 IP trisha-VirtualBox.47398 >
82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 245, win
63996, length 0
```

The first field, **18:22:49.292298** represents the timestamp of the received packet as per the local clock.

The next field, **IP** represents the network layer protocol, in this case IPv4.(For IPv6 it is specified as IP6)

The next field, **trisha-VirtualBox.47398**, is the source IP address and port
and **82.221.107.34.bc.googleusercontent.com.http** is the destination ip address and port.

After the destination, the TCP flags are specified.

The next field is the Ack Number which in this case is **245** and it specifies the next expected byte (data) on this flow. (Ack number 1 is for the side sending the data)

The next field is the window size which represents the number of bytes available in the receiving buffer which in this case is **63996**.

And lastly we have the packet length which in this example is **0**.

Step 4 : Capturing Packets based on Protocol

Capturing ICMP packets using the command :

```
sudo tcpdump -i any -c5 icmp
```

```
trisha@trisha-VirtualBox:~$ sudo tcpdump -i any -c5 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 2
62144 bytes
18:30:05.678551 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo request, id 2, seq 395, length 64
18:30:05.678563 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo reply, id 2, seq 395, length 64
18:30:06.702998 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo request, id 2, seq 396, length 64
18:30:06.703016 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo reply, id 2, seq 396, length 64
18:30:07.727085 IP trisha-VirtualBox > trisha-VirtualBox: ICMP echo request, id 2, seq 397, length 64
5 packets captured
12 packets received by filter
0 packets dropped by kernel
trisha@trisha-VirtualBox:~$
```

sudo **tcpdump -i any -c5 icmp**

Step 5 : Checking the packet content

Inspect the HTTP content of a web request using the command :

sudo **tcpdump -i any -c10 -nn -A port 80**

```
trisha@trisha-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144
bytes
18:33:52.133064 IP 10.0.2.15.47464 > 34.107.221.82.80: Flags [S], seq 3812885
594, win 64240, options [mss 1460,sackOK,TS val 3036175840 ecr 0,nop,wscale 7
], length 0
E..<./@.A.
... "k.R.h.P.D.Z.....".
[.....]
18:33:52.171933 IP 34.107.221.82.80 > 10.0.2.15.47464: Flags [S.], seq 142336
001, ack 3812885595, win 65535, options [mss 1460], length 0
E.,....@..8"k.R
....P.h.{...D.[`....u.....
18:33:52.171977 IP 10.0.2.15.47464 > 34.107.221.82.80: Flags [.], ack 1, win
64240, length 0
E..(.0@.A.
... "k.R.h.P.D.[{..P.....
18:33:52.172428 IP 10.0.2.15.47464 > 34.107.221.82.80: Flags [P.], seq 1:297,
ack 1, win 64240, length 296: HTTP: GET /success.txt HTTP/1.1
E..P.1@.A.
... "k.R.h.P.D.[{..P.....GET /success.txt HTTP/1.1
```

```
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

18:33:52.172653 IP 34.107.221.82.80 > 10.0.2.15.47464: Flags [.], ack 297, win 65535, length 0
E...(. ....@...;"k.R
....P.h.{....D..P....
.....
18:33:52.238320 IP 34.107.221.82.80 > 10.0.2.15.47464: Flags [P.], seq 1:245, ack 297, win 65535, length 244: HTTP: HTTP/1.1 200 OK
E.....@..F"k.R
....P.h.{....D..P.....HTTP/1.1 200 OK
Server: nginx
Date: Mon, 18 Jan 2021 16:52:22 GMT
Content-Type: text/plain
Via: 1.1 google
Age: 72690
Cache-Control: public, must-revalidate, max-age=0, s-maxage=86400
Content-Length: 8
Connection: keep-alive
success

18:33:52.238722 IP 10.0.2.15.47464 > 34.107.221.82.80: Flags [.], ack 245, win 63996, length 0
E...(.2@. @.A.
..."k.R.h.P.D...{..P.....
18:33:52.255769 IP 10.0.2.15.47466 > 34.107.221.82.80: Flags [S], seq 3038851270, win 64240, options [mss 1460,sackOK,TS val 3036175962 ecr 0,nop,wscale 7], length 0
E..<<3@. @...
..."k.R.j.P.!0.....
.^Z.....
18:33:52.314356 IP 34.107.221.82.80 > 10.0.2.15.47466: Flags [S.], seq 14240001, ack 3038851271, win 65535, options [mss 1460], length 0
E.,....@..1"k.R
....P.j.|....!0. ...
).....
18:33:52.314387 IP 10.0.2.15.47466 > 34.107.221.82.80: Flags [.], ack 1, win 64240, length 0
```

```
E..( .2@. @.A.  
..."k.R.h.P.D...{..P.....  
18:33:52.255769 IP 10.0.2.15.47466 > 34.107.221.82.80: Flags [S], seq 3038851  
270, win 64240, options [mss 1460,sackOK,TS val 3036175962 ecr 0,nop,wscale 7  
>, length 0  
E..<<3@. @...  
..."k.R.j.P.!0.....  
..^Z.....  
18:33:52.314356 IP 34.107.221.82.80 > 10.0.2.15.47466: Flags [S.], seq 142400  
001, ack 3038851271, win 65535, options [mss 1460], length 0  
E.,....@..1"K.R  
....P.j.|....!0.`...  
)...  
18:33:52.314387 IP 10.0.2.15.47466 > 34.107.221.82.80: Flags [.], ack 1, win  
64240, length 0  
E..(<4@. @...  
..."k.R.j.P.!0..|..P.....  
10 packets captured  
10 packets received by filter  
0 packets dropped by kernel
```

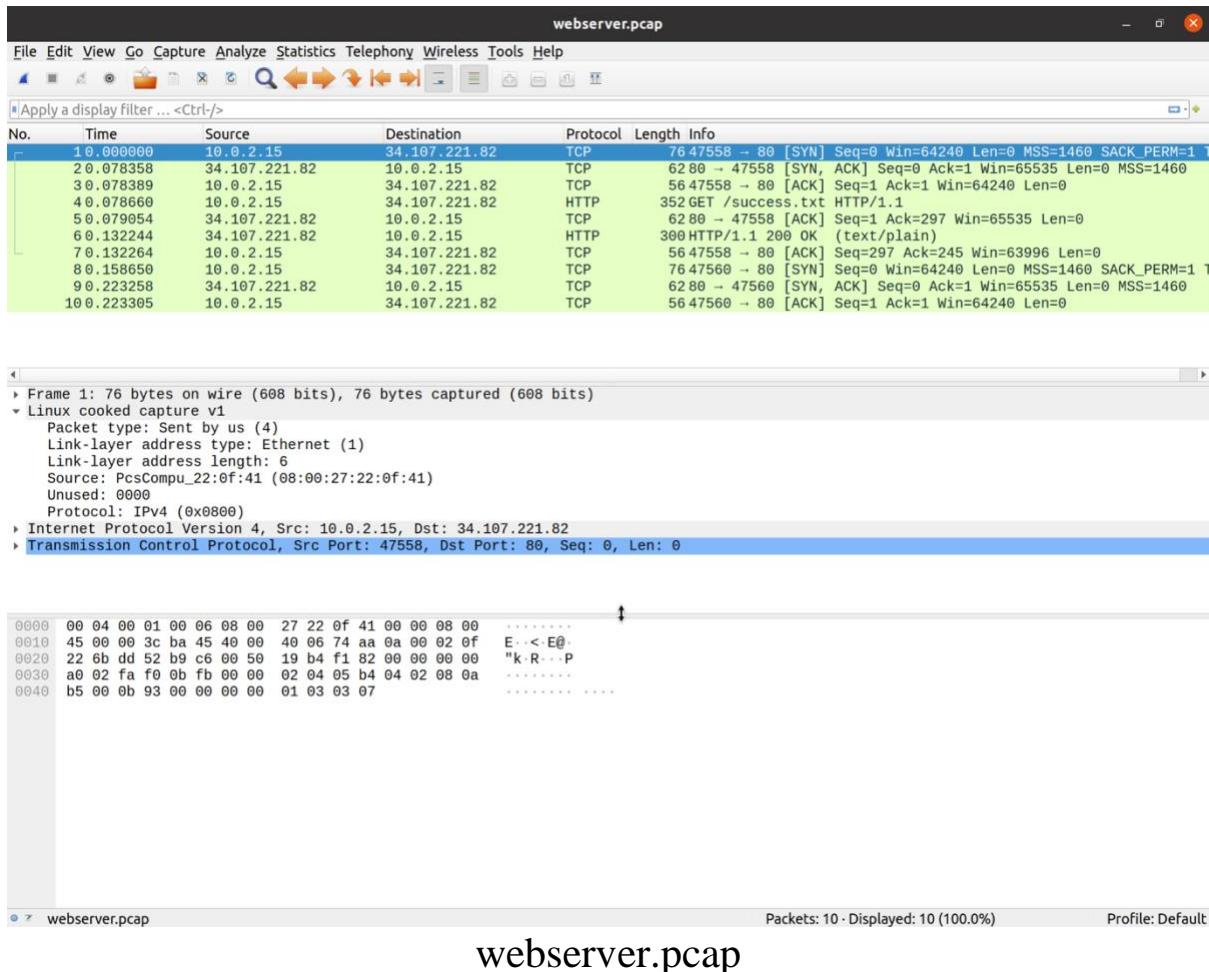
Step 6 : Saving packets to a file

Using the -w option to save the packets to a file instead of displaying them on screen,

```
sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
```

```
trisha@trisha-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -w webserver.pcap po  
rt 80  
[sudo] password for trisha:  
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture siz  
e 262144 bytes  
10 packets captured  
14 packets received by filter  
0 packets dropped by kernel  
trisha@trisha-VirtualBox:~$
```

```
sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
```



Task 5: Perform Traceroute Checks

Step 1: Running the traceroute using the command :
sudo traceroute www.google.com

```
trisha@trisha-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (172.217.31.196), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  0.286 ms  0.226 ms  0.210 ms
 2 192.168.43.97 (192.168.43.97)  13.241 ms  14.444 ms  14.429 ms
 3 * * *
 4 10.72.169.3 (10.72.169.3)  69.286 ms  69.415 ms  72.745 ms
 5 192.168.61.44 (192.168.61.44)  69.145 ms  192.168.61.46 (192.168.61.46)  69.269 ms  69.359 ms
 6 192.168.61.41 (192.168.61.41)  69.194 ms  44.983 ms  192.168.61.45 (192.168.61.45)  45.242 ms
 7 172.26.74.86 (172.26.74.86)  44.932 ms  48.900 ms  49.090 ms
 8 172.26.74.99 (172.26.74.99)  49.075 ms  29.782 ms  29.652 ms
 9 192.168.61.14 (192.168.61.14)  41.920 ms  41.644 ms  192.168.61.18 (192.168.61.18)  47.763 ms
10 192.168.61.19 (192.168.61.19)  47.998 ms  192.168.61.17 (192.168.61.17)  49.087 ms  52.215 ms
11 172.26.29.42 (172.26.29.42)  58.638 ms  56.257 ms  50.197 ms
12 172.26.29.42 (172.26.29.42)  49.665 ms  49.371 ms  172.26.29.107 (172.26.29.107)  35.062 ms
13 10.70.80.197 (10.70.80.197)  44.897 ms  32.652 ms  42.655 ms
14 10.70.80.225 (10.70.80.225)  42.746 ms  42.549 ms  47.062 ms
15 74.125.48.26 (74.125.48.26)  38.375 ms  38.001 ms  37.943 ms
16 108.170.253.97 (108.170.253.97)  55.644 ms  55.898 ms  108.170.253.113 (108.170.253.113)  49.664 ms
17 74.125.253.13 (74.125.253.13)  51.666 ms  41.615 ms  74.125.253.17 (74.125.253.17)  41.563 ms
18 maa03s28-in-f4.1e100.net (172.217.31.196)  31.787 ms  44.309 ms  56.523 ms
trisha@trisha-VirtualBox:~$
```

[sudo traceroute www.google.com](#)

Step 2: Analyzing destination address of google.com and number of hops

Number of hops : 18 (Max number of hops allowed = 30)

Destination Address of google.com : 172.217.31.196 (Destination server : maa03s28-in-f4.1e100.net)

Step 3: Speeding up the process by disabling the mapping of IP address with hostnames by using the -n option

```
trisha@trisha-VirtualBox:~$ sudo traceroute -n www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  10.0.2.2  6.447 ms  6.420 ms  6.402 ms
 2  192.168.43.97  5.688 ms  9.106 ms  9.322 ms
 3  * * *
 4  10.72.169.67  59.256 ms 10.72.169.3  59.277 ms 10.72.169.67  60.980 ms
 5  192.168.61.44  55.706 ms 192.168.61.46  57.390 ms 192.168.61.44  57.508 ms
 6  192.168.61.47  55.236 ms  54.467 ms 192.168.61.41  54.341 ms
 7  172.26.74.86  56.546 ms  56.688 ms  54.473 ms
 8  172.26.74.99  55.792 ms  36.373 ms  47.910 ms
 9  192.168.61.14  47.888 ms 192.168.61.16  54.284 ms 192.168.61.18  54.014 ms
10  192.168.61.15  57.253 ms 192.168.61.17  59.272 ms 192.168.61.15  55.926 ms
11  172.31.2.61  58.760 ms 172.31.2.67  58.546 ms  70.191 ms
12  72.14.217.252  69.932 ms 209.85.175.48  68.947 ms 72.14.211.56  36.309 ms
13  * * *
14  142.250.233.145  52.102 ms 108.170.236.196  44.516 ms  44.207 ms
15  74.125.242.146  53.141 ms 74.125.242.130  53.551 ms 142.250.71.36  51.812 ms
trisha@trisha-VirtualBox:~$
```

[**sudo traceroute -n www.google.com**](#)

Step 4: Using the -I option so that the traceroute uses ICMP

```
trisha@trisha-VirtualBox:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.251 ms  1.559 ms  5.369 ms
 2  192.168.43.97 (192.168.43.97)  10.735 ms  11.546 ms  12.187 ms
 3  * * *
 4  10.72.169.3 (10.72.169.3)  54.764 ms  55.436 ms 10.72.169.67 (10.72.169.67)  55.427 ms
 5  192.168.61.40 (192.168.61.40)  54.740 ms 192.168.61.42 (192.168.61.42)  55.418 ms 192.168.61.40 (192.
168.61.40)  55.415 ms
 6  192.168.61.41 (192.168.61.41)  54.435 ms  38.988 ms  38.951 ms
 7  172.26.74.86 (172.26.74.86)  36.314 ms  36.305 ms  37.916 ms
 8  172.26.74.99 (172.26.74.99)  38.834 ms  31.301 ms  31.272 ms
 9  192.168.61.16 (192.168.61.16)  39.265 ms 192.168.61.14 (192.168.61.14)  40.423 ms 192.168.61.16 (192.
168.61.16)  40.705 ms
10  192.168.61.15 (192.168.61.15)  39.237 ms  39.680 ms  39.823 ms
11  172.31.2.67 (172.31.2.67)  45.339 ms  45.264 ms  45.254 ms
12  72.14.217.252 (72.14.217.252)  45.248 ms  46.880 ms  43.428 ms
13  108.170.253.97 (108.170.253.97)  49.986 ms  51.238 ms  50.953 ms
14  142.250.233.145 (142.250.233.145)  51.285 ms  51.158 ms  51.146 ms
15  maa03s35-in-f4.1e100.net (142.250.71.36)  41.988 ms  45.487 ms  44.925 ms
trisha@trisha-VirtualBox:~$
```

[**sudo traceroute -I www.google.com**](#)

Step 5: Using the -T flag to test a TCP connection to gather data more relevant to web server

```
trisha@trisha-VirtualBox:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (172.217.31.196), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  0.568 ms  0.535 ms  0.497 ms
 2 maa03s28-in-f4.1e100.net (172.217.31.196)  45.316 ms  57.527 ms  39.568 ms
trisha@trisha-VirtualBox:~$ █
```

sudo **traceroute -T www.google.com**

Task 6: Explore an entire network for information (nmap)

Step 1: Scanning a host using host name (Command: nmap www.pes.edu)

```
trisha@trisha-VirtualBox:~$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-25 14:57 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.016s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
```

Step 2: Scanning a host using IP Address

Command used : [nmap 163.53.78.128](#)

```
trisha@trisha-VirtualBox:~$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-25 14:57 IST
Nmap scan report for 163.53.78.128
Host is up (0.17s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 42.35 seconds
```

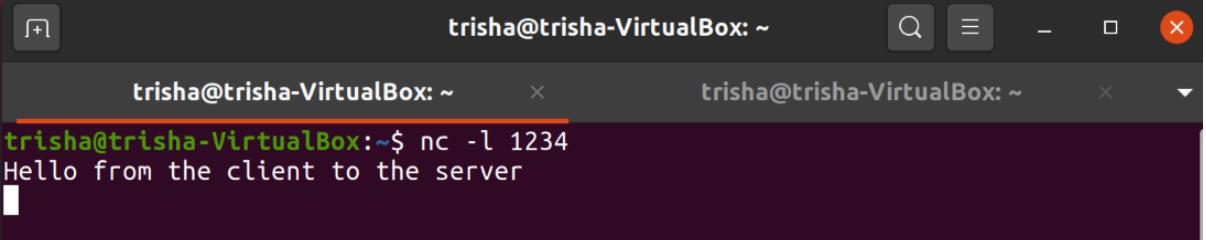
Step 3: Scanning multiple IP Addresses

Command used : [nmap 192.168.1.1 192.168.1.2 192.168.1.3](#)

```
trisha@trisha-VirtualBox:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-25 14:58 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.09 seconds
```

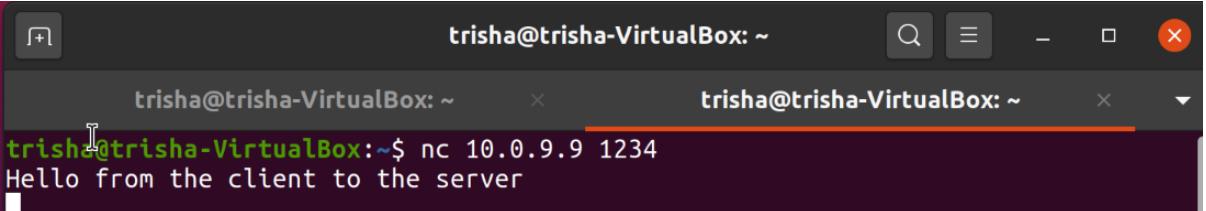
Task 7 a): Netcat as Chat tool

- a) Intra system communication (Using 2 terminals in the same system)



```
trisha@trisha-VirtualBox:~$ nc -l 1234
Hello from the client to the server
```

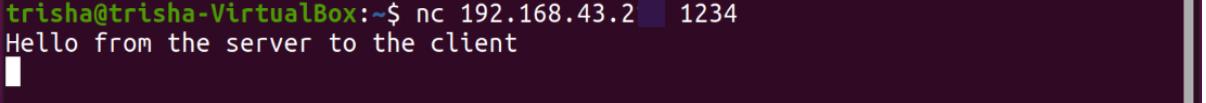
nc -l 1234



```
trisha@trisha-VirtualBox:~$ nc 10.0.9.9 1234
Hello from the client to the server
```

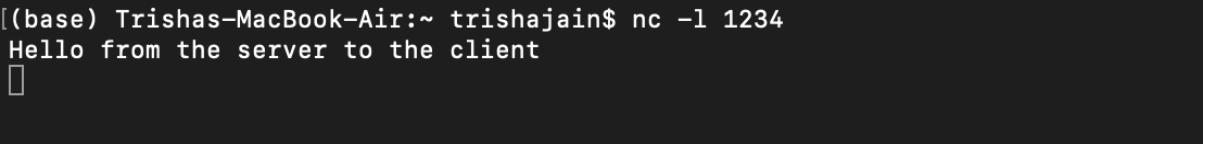
nc 10.0.9.9 1234

- b) Inter system communication



```
trisha@trisha-VirtualBox:~$ nc 192.168.43.2 1234
Hello from the server to the client
```

nc 192.168.43.2?? 1234

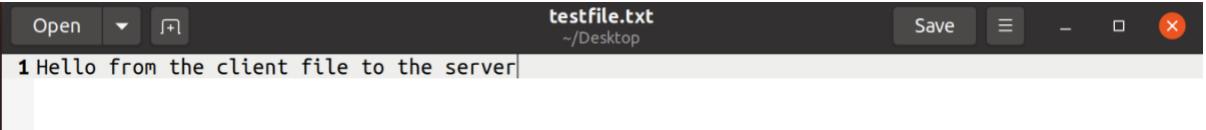


```
(base) Trishas-MacBook-Air:~ trishajain$ nc -l 1234
Hello from the server to the client
```

nc -l 1234

Note: The last two digits of the IP address have been hidden.

Task 7 b): Use Netcat to transfer files



```
testfile.txt
~/Desktop
1 Hello from the client file to the server
```

testfile.txt

```
trisha@trisha-VirtualBox:~/Desktop$ sudo nc 192.168.43.2 555 < testfile.txt  
trisha@trisha-VirtualBox:~/Desktop$
```

sudo nc 192.168.43.2?? 555 < testfile.txt

```
[(base) Trishas-MacBook-Air:Desktop trishajain$ sudo nc -l 555 > test.txt  
[Password:
```

```
[(base) Trishas-MacBook-Air:Desktop trishajain$ cat test.txt  
Hello from the client file to the server
```

sudo nc -l 555 > test.txt

Task 7 c): Other commands

- 1) To test if a TCP port of a remote host is open

The screenshot shows two terminal windows side-by-side. The top window has the command `nc -l 1234` running, indicated by a blank line with a cursor. The bottom window has two commands: `nc -vn 10.0.2.15 555` which failed with a connection refused error, and `nc -vn 10.0.2.15 1234` which succeeded.

```
trisha@trisha-VirtualBox:~/Desktop$ nc -l 1234  
trisha@trisha-VirtualBox:~/Desktop$ nc -vn 10.0.2.15 555  
nc: connect to 10.0.2.15 port 555 (tcp) failed: Connection refused  
trisha@trisha-VirtualBox:~/Desktop$ nc -vn 10.0.2.15 1234  
Connection to 10.0.2.15 1234 port [tcp/*] succeeded!
```

`nc -vn 10.0.2.15 555`

- 2) Run a web server with a static web page

```
trisha@trisha-VirtualBox:~/Desktop$ while true; do sudo nc -lp 80 < test.html; done  
GET /test.html HTTP/1.1  
Host: 10.0.2.15  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1
```

while `true`; do `sudo nc -lp 80 < test.html; done`

Questions on above observations:-

Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?

A1. The browser is running HTTP version 1.1.

```
Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.flipkart.com\r\n
HTTP 1.1 for request
```

The server is also running HTTP version 1.1.

```
  ▶ Hypertext Transfer Protocol
    ▶ HTTP/1.1 301 Moved Permanently\r\n
      Server: nginx\r\n
HTTP 1.1 for response
```

Q2. When was the HTML file that you are retrieving last modified at the server?

A2. The date the HTML file was last modified is specified in the Last-Modified field.

```
  ▶ Hypertext Transfer Protocol
    ▶ HTTP/1.1 200 OK\r\n
      Server: nginx/1.14.0 (Ubuntu)\r\n
      Date: Sun, 24 Jan 2021 11:38:36 GMT\r\n
      Content-Type: application/octet-stream\r\n
    ▶ Content-Length: 76444\r\n
      Last-Modified: Tue, 08 Dec 2020 16:13:54 GMT\r\n
Specified as Tue, 08 Dec 2020 16:13:54 GMT\r\n
```

Q3. How to tell ping to exit after a specified number of ECHO_REQUEST packets?

A3. The ICMP packages continue to be sent until interrupted. Therefore to exit after a specified number of ECHO_REQUEST packets, we can use the -c option followed by the number of packets.

Q4. How will you identify remote host apps and OS?

A4. The remote host apps and OS can be identified using the command as shown below:

```
trisha@trisha-VirtualBox:~$ sudo nmap -O -v www.flipkart.com
[sudo] password for trisha:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-25 11:34 IST
Initiating Ping Scan at 11:34
Scanning www.flipkart.com (163.53.76.86) [4 ports]
Completed Ping Scan at 11:34, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:34
Completed Parallel DNS resolution of 1 host. at 11:34, 0.01s elapsed
Initiating SYN Stealth Scan at 11:34
Scanning www.flipkart.com (163.53.76.86) [1000 ports]
Discovered open port 1723/tcp on 163.53.76.86
Discovered open port 554/tcp on 163.53.76.86
Discovered open port 21/tcp on 163.53.76.86
Discovered open port 443/tcp on 163.53.76.86
Discovered open port 80/tcp on 163.53.76.86
Completed SYN Stealth Scan at 11:35, 15.16s elapsed (1000 total ports)
Initiating OS detection (try #1) against www.flipkart.com (163.53.76.86)
Nmap scan report for www.flipkart.com (163.53.76.86)
Host is up (0.014s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.18 seconds
Raw packets sent: 3033 (135.720KB) | Rcvd: 35 (1.512KB)
```

`sudo nmap -O -v www.flipkart.com`