

# Week 1

|                  |                    |
|------------------|--------------------|
| NAME : SUNDEEP A | SRN: PES1UG20CS445 |
| ROLL NO: 48      | SECTION: H         |

## Task 1: Linux Interface configuration(ifconfig/IP command)

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

| Interface name | IP address   | MAC address       |
|----------------|--|-------------------|
| Ens33          | IPv4 - 192.168.100.138<br>IPv6 - fe80::d1ff:29cb:a3b2:8064 | 00:0c:29:f9:4f:7d |
| lo             | IPv4 – 127.0.0.1<br>IPv6 - ::1                             | 00:0c:29:f9:4f:7d |

```
pes1ug20cs445@sundeep:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.138 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::d1ff:29cb:a3b2:8064 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f9:4f:7d txqueuelen 1000 (Ethernet)
    RX packets 6783 bytes 9371223 (9.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1911 bytes 160922 (160.9 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 267 bytes 26141 (26.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 267 bytes 26141 (26.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step 2: To assign my IP address:

```
pes1ug20cs445@sundeep:~/Desktop$ sudo ifconfig ens33 10.0.8.48 netmask 255.255.255.0
pes1ug20cs445@sundeep:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.8.48 netmask 255.255.255.0 broadcast 10.0.8.255
    inet6 fe80::d1ff:29cb:a3b2:8064 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f9:4f:7d txqueuelen 1000 (Ethernet)
    RX packets 51351 bytes 69790443 (69.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15405 bytes 1132022 (1.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Command used is – sudo ifconfig ens33 10.0.8.48 netmask 255.255.255.0

So, In the screenshot we can see that the IP address has been changed

Step 3: To activate and deactivate a network interface, type:

Deactivating ens33:

```

pes1ug20cs445@sundeeep:~/Desktop$ sudo ifconfig ens33 down
pes1ug20cs445@sundeeep:~/Desktop$ 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 1328 bytes 129887 (129.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1328 bytes 129887 (129.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

pes1ug20cs445@sundeeep:~/Desktop$

```

Thus, ens33 has been successfully deactivated

Activating ens33:

```

pes1ug20cs445@sundeeep:~/Desktop$ sudo ifconfig ens33 up
pes1ug20cs445@sundeeep:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.138 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::diff:29cb:a3b2:8064 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f9:4f:7d txqueuelen 1000 (Ethernet)
    RX packets 51650 bytes 69844246 (69.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15569 bytes 1153295 (1.1 MB)
    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 1610 bytes 157125 (157.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1610 bytes 157125 (157.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

pes1ug20cs445@sundeeep:~/Desktop$

```

Step 4: To show the current neighbor

```

pes1ug20cs445@sundeeep:~/Desktop$ ip neigh
192.168.100.2 dev ens33 lladdr 00:50:56:e6:5a:60 REACHABLE
pes1ug20cs445@sundeeep:~/Desktop$

```

## Task 2: Ping PDU Capture

Step 1: Assign an IP address to the system.

```

pes1ug20cs445@sundeeep:~/Desktop$ sudo ifconfig ens33 10.0.8.48 netmask 255.255.255.0
pes1ug20cs445@sundeeep:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.8.48 netmask 255.255.255.0 broadcast 10.0.8.255
    inet6 fe80::diff:29cb:a3b2:8064 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f9:4f:7d txqueuelen 1000 (Ethernet)
    RX packets 51351 bytes 69790443 (69.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15405 bytes 1132022 (1.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Step 2: Launch Wireshark and select 'any' interface

| Apply a display filter ... <Ctrl-/> |             |                        |                 |          |        |   |
|-------------------------------------|-------------|------------------------|-----------------|----------|--------|---|
| No.                                 | Time        | Source                 | Destination     | Protocol | Length | Info  |
| 1                                   | 0.000000000 | 192.168.100.1          | 192.168.100.255 | UDP      | 186    | 60121 → 51007 Len=144   |
| 2                                   | 0.367805349 | 192.168.100.138        | 192.168.100.2   | DNS      | 76     | Standard query 0xe5c2 A wpad.localdomain                        |
| 3                                   | 0.370130664 | 192.168.100.1          | 224.0.0.251     | MDNS     | 70     | Standard query 0x0000 A wpad.local, "QM" question               |
| 4                                   | 0.370825296 | fe80::a14d:624:9d6d... | ff02::fb        | MDNS     | 90     | Standard query 0x0000 A wpad.local, "QM" question               |
| 5                                   | 0.373708844 | 192.168.100.1          | 224.0.0.251     | MDNS     | 70     | Standard query 0x0000 A wpad.local, "QM" question               |
| 6                                   | 0.374389844 | fe80::a14d:624:9d6d... | ff02::fb        | MDNS     | 90     | Standard query 0x0000 A wpad.local, "QM" question               |
| 7                                   | 0.376170279 | fe80::a14d:624:9d6d... | ff02::1:3       | LLMNR    | 84     | Standard query 0x8e21 A wpad                                    |
| 8                                   | 0.376170485 | 192.168.100.1          | 224.0.0.252     | LLMNR    | 64     | Standard query 0x8e21 A wpad                                    |
| 9                                   | 0.595705241 | 192.168.100.138        | 192.168.100.2   | ICMP     | 98     | Echo (ping) request id=0x0003, seq=24/6144, ttl=64 (reply in... |
| 10                                  | 0.596227930 | 192.168.100.2          | 192.168.100.138 | ICMP     | 98     | Echo (ping) reply id=0x0003, seq=24/6144, ttl=128 (request...   |
| 11                                  | 0.787603677 | fe80::a14d:624:9d6d... | ff02::1:3       | LLMNR    | 84     | Standard query 0x8e21 A wpad                                    |
| 12                                  | 0.787604448 | 192.168.100.1          | 224.0.0.252     | LLMNR    | 64     | Standard query 0x8e21 A wpad                                    |
| 13                                  | 1.370050313 | 192.168.100.1          | 224.0.0.251     | MDNS     | 70     | Standard query 0x0000 A wpad.local, "QM" question               |
| 14                                  | 1.370963278 | fe80::a14d:624:9d6d... | ff02::fb        | MDNS     | 90     | Standard query 0x0000 A wpad.local, "QM" question               |
| 15                                  | 1.373952264 | 192.168.100.1          | 224.0.0.251     | MDNS     | 70     | Standard query 0x0000 A wpad.local, "QM" question               |
| 16                                  | 1.374878953 | fe80::a14d:624:9d6d... | ff02::fb        | MDNS     | 90     | Standard query 0x0000 A wpad.local, "QM" question               |
| 17                                  | 1.620208793 | 192.168.100.138        | 192.168.100.2   | ICMP     | 98     | Echo (ping) request id=0x0003, seq=25/6400, ttl=64 (reply in... |
| 18                                  | 1.620734880 | 192.168.100.2          | 192.168.100.138 | ICMP     | 98     | Echo (ping) reply id=0x0003, seq=25/6400, ttl=128 (request...   |
| 19                                  | 1.949183043 | 192.168.100.1          | 239.255.255.250 | SSDP     | 179    | M-SEARCH * HTTP/1.1   |

▶ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens33, id 0  
 ▶ Ethernet II, Src: VMware\_f9:4f:7d (00:0c:29:f9:4f:7d), Dst: VMware\_e6:5a:60 (00:50:56:e6:5a:60)  
 ▶ Internet Protocol Version 4, Src: 192.168.100.138, Dst: 192.168.100.2  
 ▶ Internet Control Message Protocol

Step 3: In terminal, type ping 10.0.your\_section.your\_sno

```

pesiug20cs445@sundeep:~/Desktop$ ping 10.0.8.48
PING 10.0.8.48 (10.0.8.48) 56(84) bytes of data.
64 bytes from 10.0.8.48: icmp_seq=1 ttl=64 time=0.107 ms
64 bytes from 10.0.8.48: icmp_seq=2 ttl=64 time=0.105 ms
64 bytes from 10.0.8.48: icmp_seq=3 ttl=64 time=0.031 ms
64 bytes from 10.0.8.48: icmp_seq=4 ttl=64 time=0.032 ms
64 bytes from 10.0.8.48: icmp_seq=5 ttl=64 time=0.036 ms
64 bytes from 10.0.8.48: icmp_seq=6 ttl=64 time=0.032 ms
64 bytes from 10.0.8.48: icmp_seq=7 ttl=64 time=0.094 ms
64 bytes from 10.0.8.48: icmp_seq=8 ttl=64 time=0.117 ms
64 bytes from 10.0.8.48: icmp_seq=9 ttl=64 time=0.048 ms
64 bytes from 10.0.8.48: icmp_seq=10 ttl=64 time=0.086 ms
64 bytes from 10.0.8.48: icmp_seq=11 ttl=64 time=0.085 ms
64 bytes from 10.0.8.48: icmp_seq=12 ttl=64 time=0.053 ms
64 bytes from 10.0.8.48: icmp_seq=13 ttl=64 time=0.052 ms
64 bytes from 10.0.8.48: icmp_seq=14 ttl=64 time=0.080 ms
64 bytes from 10.0.8.48: icmp_seq=15 ttl=64 time=0.150 ms
^C
--- 10.0.8.48 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14337ms
rtt min/avg/max/mdev = 0.031/0.073/0.150/0.035 ms
pesiug20cs445@sundeep:~/Desktop$
  
```

Step 4: Observations to be made

|                       |                    |
|-----------------------|--------------------|
| TTL                   | 64                 |
| Protocol Used By Ping | ICMP               |
| Time                  | Order of $10^{-2}$ |

Step 5: Analyze the following in Wireshark

I am pinging my neighbor's system

HTTP Request:

| No.  | Time        | Source          | Destination     | Protocol | Length | Info  |
|--|-------------|-----------------|-----------------|----------|--------|---|
| 2  | 0.367805349 | 192.168.100.138 | 192.168.100.2   | DNS      | 76     | Standard query 0xe5c2 A wpad.localdomain                        |
| 9  | 0.595705241 | 192.168.100.138 | 192.168.100.2   | ICMP     | 98     | Echo (ping) request id=0x0003, seq=24/6144, ttl=64 (reply in... |
| 10   | 0.596227930 | 192.168.100.2   | 192.168.100.138 | ICMP     | 98     | Echo (ping) reply id=0x0003, seq=24/6144, ttl=128 (request...   |
| 17   | 1.620208793 | 192.168.100.138 | 192.168.100.2   | ICMP     | 98     | Echo (ping) request id=0x0003, seq=25/6400, ttl=64 (reply in... |
| 18   | 1.620734880 | 192.168.100.2   | 192.168.100.138 | ICMP     | 98     | Echo (ping) reply id=0x0003, seq=25/6400, ttl=128 (request...   |
| ▼ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens33, id 0 <ul style="list-style-type: none"> <li>Interface id: 0 (ens33)               <ul style="list-style-type: none"> <li>Encapsulation type: Ethernet (1)                   <ul style="list-style-type: none"> <li>Arrival Time: Jan 25, 2022 12:31:29.722784030 IST</li> <li>[Time shift for this packet: 0.000000000 seconds]</li> <li>Epoch Time: 1643094089.722784030 seconds</li> <li>[Time delta from previous captured frame: 0.219534756 seconds]</li> <li>[Time delta from previous displayed frame: 0.227899892 seconds]</li> <li>[Time since reference or first frame: 0.595705241 seconds]</li> <li>Frame Number: 9</li> <li>Frame Length: 98 bytes (784 bits)</li> <li>Capture Length: 98 bytes (784 bits)</li> <li>[Frame is marked: False]</li> <li>[Frame is ignored: False]</li> <li>[Protocols in frame: eth:ethertype:ip:icmp:data]</li> <li>[Coloring Rule Name: ICMP]</li> <li>[Coloring Rule String: icmp    icmpv6]</li> </ul> </li> </ul> </li> </ul> |             |                 |                 |          |        |   |
| ▼ Ethernet II, Src: VMware_f9:4f:7d (00:0c:29:f9:4f:7d), Dst: VMware_e6:5a:60 (00:50:56:e6:5a:60) <ul style="list-style-type: none"> <li>Destination: VMware_e6:5a:60 (00:50:56:e6:5a:60)</li> <li>Source: VMware_f9:4f:7d (00:0c:29:f9:4f:7d)</li> <li>Type: IPv4 (0x0800)</li> </ul>   |             |                 |                 |          |        |   |
| ▼ Internet Protocol Version 4, Src: 192.168.100.138, Dst: 192.168.100.2 <ul style="list-style-type: none"> <li>0100 .... = Version: 4</li> <li>.... 0101 = Header Length: 20 bytes (5)</li> <li>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</li> <li>Total Length: 84</li> <li>Identification: 0x59fe (23038)</li> <li>Flags: 0x4000, Don't fragment</li> <li>Fragment offset: 0</li> <li>Time to live: 64</li> <li>Protocol: ICMP (1)</li> <li>Header checksum: 0x96cd [validation disabled]</li> <li>[Header checksum status: Unverified]</li> <li>Source: 192.168.100.138</li> <li>Destination: 192.168.100.2</li> </ul>  |             |                 |                 |          |        |   |
| ▼ Internet Control Message Protocol <ul style="list-style-type: none"> <li>Type: 8 (Echo (ping) request)</li> <li>Code: 0</li> <li>Checksum: 0xd308 [correct]</li> <li>[Checksum Status: Good]</li> <li>Identifier (BE): 3 (0x0003)</li> <li>Identifier (LE): 768 (0x0300)</li> <li>Sequence number (BE): 24 (0x0018)</li> <li>Sequence number (LE): 6144 (0x1800)</li> </ul>  |             |                 |                 |          |        |   |

## HTTP Response:

| No.  | Time        | Source          | Destination     | Protocol | Length | Info  |
|--|-------------|-----------------|-----------------|----------|--------|---|
| 2  | 0.367805349 | 192.168.100.138 | 192.168.100.2   | DNS      | 76     | Standard query 0xe5c2 A wpad.localdomain                        |
| 9  | 0.595705241 | 192.168.100.138 | 192.168.100.2   | ICMP     | 98     | Echo (ping) request id=0x0003, seq=24/6144, ttl=64 (reply in... |
| 10   | 0.596227930 | 192.168.100.2   | 192.168.100.138 | ICMP     | 98     | Echo (ping) reply id=0x0003, seq=24/6144, ttl=128 (request...   |
| 17   | 1.620208793 | 192.168.100.138 | 192.168.100.2   | ICMP     | 98     | Echo (ping) request id=0x0003, seq=25/6400, ttl=64 (reply in... |
| 18   | 1.620734880 | 192.168.100.2   | 192.168.100.138 | ICMP     | 98     | Echo (ping) reply id=0x0003, seq=25/6400, ttl=128 (request...   |
| ▼ Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens33, id 0 <ul style="list-style-type: none"> <li>Interface id: 0 (ens33)               <ul style="list-style-type: none"> <li>Encapsulation type: Ethernet (1)                   <ul style="list-style-type: none"> <li>Arrival Time: Jan 25, 2022 12:31:29.723306719 IST</li> <li>[Time shift for this packet: 0.000000000 seconds]</li> <li>Epoch Time: 1643094089.723306719 seconds</li> <li>[Time delta from previous captured frame: 0.000522689 seconds]</li> <li>[Time delta from previous displayed frame: 0.000522689 seconds]</li> <li>[Time since reference or first frame: 0.596227930 seconds]</li> <li>Frame Number: 10</li> <li>Frame Length: 98 bytes (784 bits)</li> <li>Capture Length: 98 bytes (784 bits)</li> <li>[Frame is marked: False]</li> <li>[Frame is ignored: False]</li> <li>[Protocols in frame: eth:ethertype:ip:icmp:data]</li> <li>[Coloring Rule Name: ICMP]</li> <li>[Coloring Rule String: icmp    icmpv6]</li> </ul> </li> </ul> </li> </ul> |             |                 |                 |          |        |   |
| ▼ Ethernet II, Src: VMware_e6:5a:60 (00:50:56:e6:5a:60), Dst: VMware_f9:4f:7d (00:0c:29:f9:4f:7d) <ul style="list-style-type: none"> <li>Destination: VMware_f9:4f:7d (00:0c:29:f9:4f:7d)</li> <li>Source: VMware_e6:5a:60 (00:50:56:e6:5a:60)</li> <li>Type: IPv4 (0x0800)</li> </ul>   |             |                 |                 |          |        |   |
| ▼ Internet Protocol Version 4, Src: 192.168.100.2, Dst: 192.168.100.138 <ul style="list-style-type: none"> <li>0100 .... = Version: 4</li> <li>.... 0101 = Header Length: 20 bytes (5)</li> <li>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</li> <li>Total Length: 84</li> <li>Identification: 0xffe6 (65510)</li> <li>Flags: 0x0000</li> <li>Fragment offset: 0</li> <li>Time to live: 128</li> <li>Protocol: ICMP (1)</li> <li>Header checksum: 0xf0e4 [validation disabled]</li> <li>[Header checksum status: Unverified]</li> <li>Source: 192.168.100.2</li> <li>Destination: 192.168.100.138</li> </ul>   |             |                 |                 |          |        |   |
| ▼ Internet Control Message Protocol <ul style="list-style-type: none"> <li>Type: 0 (Echo (ping) reply)</li> <li>Code: 0</li> <li>Checksum: 0xdb08 [correct]</li> <li>[Checksum Status: Good]</li> <li>Identifier (BE): 3 (0x0003)</li> <li>Identifier (LE): 768 (0x0300)</li> <li>Sequence number (BE): 24 (0x0018)</li> <li>Sequence number (LE): 6144 (0x1800)</li> </ul>  |             |                 |                 |          |        |   |

| Details                | First Request   | First Reply     |
|------------------------|-----------------|-----------------|
| Frame Number           | 9               | 10              |
| Source IP address      | 192.168.100.138 | 192.168.100.2   |
| Destination IP address | 192.168.100.2   | 192.168.100.138 |
| ICMP Type Value        | 8               | 0               |

|                              |                   |                   |
|------------------------------|-------------------|-------------------|
| ICMP Code Value              | 0                 | 0                 |
| Source Ethernet Address      | 00:0c:29:f9:4f:7d | 00:50:56:e6:5a:60 |
| Destination Ethernet Address | 00:50:56:e6:5a:60 | 00:0c:29:f9:4f:7d |
| Internet Protocol Version    | 4                 | 4                 |
| Time To Live Value           | 64                | 128               |

### Task 3: HTTP PDU Capture

Since Flipkart.com is a https protocol , I have used info.cern.ch website which has http protocol.

#### Http Request:

```

▼ Frame 17: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface ens33, id 0
  ► Interface id: 0 (ens33)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2022 22:15:56.872827889 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1643042756.872827889 seconds
    [Time delta from previous captured frame: 0.000862703 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 6.263798992 seconds]
    Frame Number: 17
    Frame Length: 542 bytes (4336 bits)
    Capture Length: 542 bytes (4336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  ▼ Ethernet II, Src: VMWare_f9:4f:7d (00:0c:29:f9:4f:7d), Dst: VMWare_e6:5a:60 (00:50:56:e6:5a:60)
    ► Destination: VMWare_e6:5a:60 (00:50:56:e6:5a:60)
    ► Source: VMWare_f9:4f:7d (00:0c:29:f9:4f:7d)
    Type: IPv4 (0x0800)
  ▼ Internet Protocol Version 4, Src: 192.168.100.138, Dst: 188.184.21.108
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 528
      Identification: 0xf6c (64364)
    ► Flags: 0x4000, Don't fragment
      Fragment offset: 0
      Time to live: 64
      Protocol: TCP (6)
      Header checksum: 0x4624 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.100.138
      Destination: 188.184.21.108
    ► Transmission Control Protocol, Src Port: 59172, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
  ▼ Hypertext Transfer Protocol
    ► GET / HTTP/1.1\r\n
      Host: info.cern.ch\r\n
      User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Referer: https://www.google.com/\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      If-Modified-Since: Wed, 05 Feb 2014 16:00:31 GMT\r\n
      If-None-Match: "286-4f1adb3105c0"\r\n
      Cache-Control: max-age=0\r\n
      \r\n
      [Full request URI: https://info.cern.ch/]
0030 fa f0 f9 59 00 00 47 45 54 20 2f 20 48 54 54 50  ...Y...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 6e 66 6f  /1.1--Ho st: info
0050 2e 63 65 72 6e 2e 63 68 0d 0a 55 73 65 72 2d 43  .cern.ch --User-A

```

#### Http response:

```

Frame 21: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface ens33, id 0
  Interface id: 0 (ens33)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2022 22:15:57.201117459 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1643042757.201117459 seconds
    [Time delta from previous captured frame: 0.028424724 seconds]
    [Time delta from previous displayed frame: 0.328289570 seconds]
    [Time since reference or first frame: 6.592088562 seconds]
    Frame Number: 21
    Frame Length: 182 bytes (1456 bits)
    Capture Length: 182 bytes (1456 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  Ethernet II, Src: VMware_e6:5a:60 (00:50:56:e6:5a:60), Dst: VMware_f9:4f:7d (00:0c:29:f9:4f:7d)
    Destination: VMware_f9:4f:7d (00:0c:29:f9:4f:7d)
    Source: VMware_e6:5a:60 (00:50:56:e6:5a:60)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.100.138
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 168
    Identification: 0x77f7 (30711)
    Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xcb01 [validation disabled]
    [Header checksum status: Unverified]
    Source: 188.184.21.108
    Destination: 192.168.100.138
  Transmission Control Protocol, Src Port: 80, Dst Port: 59172, Seq: 1, Ack: 489, Len: 128
  Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Mon, 24 Jan 2022 16:45:56 GMT\r\n
    Server: Apache\r\n
    Connection: close\r\n
    ETag: "286-4f1adb3105c0"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.328289570 seconds]
    [Request in frame: 17]
    [Request URI: http://info.cern.ch/]

```

```

0030 fa f0 c5 40 00 00 48 54 54 50 2f 31 2e 31 20 33 ...@..HT TP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 34 Not Modified-
0050 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 34 20 4a .Date: Mon, 24 J

```

Step 3: Analyze the first (interaction of host to the web server) and second frame (response of server to the client).

| Details                      | First Echo Request | First Echo Response |
|------------------------------|--------------------|---------------------|
| Frame Number                 | 17                 | 21                  |
| Source IP address            | 192.168.100.138    | 188.184.21.108      |
| Destination IP address       | 188.184.21.108     | 192.168.100.138     |
| Source Port                  | 59172              | 80                  |
| Destination Port             | 80                 | 59172               |
| Source Ethernet Address      | 00:0c:29:f9:f4:7d  | 00:50:56:e6:5a:60   |
| Destination Ethernet Address | 00:50:56:e6:5a:60  | 00:0c:29:f9:f4:7d   |

Step 4: Analyze the HTTP request and response and complete the table.

```

Host: ocsp.digicert.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101
Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

0Q00M0K0I0..+.....+.....v.....$....8..
..)....9mz..3.....z.....+t6.{10.T0.].HTTP/1.1 200 OK
Accept-Ranges: bytes
Age: 3372
Cache-Control: max-age=127316
Content-Type: application/ocsp-response
Date: Mon, 24 Jan 2022 18:11:30 GMT
Etag: "61ee2cfa-139"
Expires: Wed, 26 Jan 2022 05:33:26 GMT
Last-Modified: Mon, 24 Jan 2022 04:37:14 GMT
Server: ECS (nag/998C)
X-Cache: HIT
Content-Length: 313

0..5
.....0..*..+.....0.....0.....0.....
..)....9mz..3.....z.....20220124043714Z0s0q0I0 ..+.....+.....v.....$....8..
..)....9mz..3.....z.....+t6.{10.T0.].20220124042102Z.....20220131033602Z0
..*.H.=...h.0e.0....0...:..ty.c..y+./..IC...].1.....+q5...s.P.....

```

| HTTP Request    |   | HTTP Response  |                           |
|-----------------|---|----------------|---------------------------|
| Get             | GET / HTTP/1.1                                | Server         | ECS(nag/998C)             |
| Host            | ocsp.digicert.com                             | Content-Type   | Application/ocsp-response |
| Accept-Language | En-US   | Date           | 24 jan 2022 5:33:26 GMT   |
| Accept-Encoding | gzip,deflate                                  | Location       | ocsp.digicert.com         |
| Connection      | Keep-alive                                    | Connection     | Keep-alive                |
| User-agent      | Mozilla/5.0<br>Gecko/20100101<br>Firefox/96.0 | Content length | 313                       |

#### Task 4: Capturing Packets with TCP dump

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

```

pes1ug20cs445@sundeep: ~/Desktop
pes1ug20cs445@sundeep:~/Desktop$ sudo tcpdump -D
[sudo] password for pes1ug20cs445:
1.ens33 [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]
pes1ug20cs445@sundeep:~/Desktop$

```

Step 2: Capture all packets in any interface



```

pesiug20cs445@sundeep:~/Desktop$ sudo tcpdump -i any
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
23:58:00.187745 IP sundeep > bom07s24-in-f4.1e100.net: ICMP echo request, id 1, seq 19, length 64
23:58:00.189699 IP localhost.41506 > localhost.domain: 12249+ [1au] PTR? 228.67.250.142.in-addr.arpa. (56)
23:58:00.190430 IP sundeep.60834 > _gateway.domain: 64120+ PTR? 228.67.250.142.in-addr.arpa. (45)
23:58:00.224504 IP bom07s24-in-f4.1e100.net > sundeep: ICMP echo reply, id 1, seq 19, length 64
23:58:00.226969 IP _gateway.domain > sundeep.60834: 64120 1/0/0 PTR bom07s24-in-f4.1e100.net. (83)
23:58:00.227486 IP localhost.domain > localhost.41506: 12249 1/0/1 PTR bom07s24-in-f4.1e100.net. (94)
23:58:00.265143 IP localhost.59583 > localhost.domain: 25953+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
23:58:01.190483 IP sundeep > bom07s24-in-f4.1e100.net: ICMP echo request, id 1, seq 20, length 64
23:58:01.225410 IP bom07s24-in-f4.1e100.net > sundeep: ICMP echo reply, id 1, seq 20, length 64
23:58:01.534913 IP 192.168.100.1.60856 > 192.168.100.255.51007: UDP, length 144
23:58:01.535399 IP localhost.36949 > localhost.domain: 56936+ [1au] PTR? 255.100.168.192.in-addr.arpa. (57)
23:58:01.536097 IP sundeep.52425 > _gateway.domain: 53906+ PTR? 255.100.168.192.in-addr.arpa. (46)
23:58:01.570889 IP _gateway.domain > sundeep.52425: 53906 NXDomain 0/1/0 (95)
23:58:01.571599 IP localhost.domain > localhost.36949: 56936 NXDomain 0/0/1 (57)
^C
14 packets captured
39 packets received by filter
18 packets dropped by kernel
pesiug20cs445@sundeep:~/Desktop$

```

Step 3: To filter packets based on protocol, specifying the protocol in the command line. For example, capture ICMP packets

```

pesiug20cs445@sundeep:~/Desktop$ 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 262144 bytes
23:59:56.190219 IP sundeep > bom07s24-in-f4.1e100.net: ICMP echo request, id 2, seq 6, length 64
23:59:56.227229 IP bom07s24-in-f4.1e100.net > sundeep: ICMP echo reply, id 2, seq 6, length 64
23:59:57.192436 IP sundeep > bom07s24-in-f4.1e100.net: ICMP echo request, id 2, seq 7, length 64
23:59:57.229243 IP bom07s24-in-f4.1e100.net > sundeep: ICMP echo reply, id 2, seq 7, length 64
23:59:58.194246 IP sundeep > bom07s24-in-f4.1e100.net: ICMP echo request, id 2, seq 8, length 64
5 packets captured
5 packets received by filter
0 packets dropped by kernel
pesiug20cs445@sundeep:~/Desktop$

```

Step 4: : Check the packet content. For example, inspect the HTTP content of a web request

```

pesiug20cs445@sundeep:~/Desktop$ 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
00:01:57.958225 IP 192.168.100.138.45396 > 35.232.111.17.80: Flags [S], seq 886004043, win 64240, options [mss 1460,sackOK,TS val 137418184 ecr 0,nop,wscale 7], length 0
E..A.@.A...d.#.o..T.P4.YK.....Z.....
..0.....
00:01:58.974062 IP 192.168.100.138.45396 > 35.232.111.17.80: Flags [S], seq 886004043, win 64240, options [mss 1460,sackOK,TS val 137419200 ecr 0,nop,wscale 7], length 0
E..A.@.A...d.#.o..T.P4.YK.....Z.....
..0.....
00:01:59.250099 IP 35.232.111.17.80 > 192.168.100.138.45396: Flags [S.], seq 1259145604, ack 886004044, win 64240, options [mss 1460], length 0
E...t.....#..o...d..P.TK. .4.Y.P...P.....
00:01:59.250259 IP 192.168.100.138.45396 > 35.232.111.17.80: Flags [.], ack 1, win 64240, length 0
E..(A.@.A...d.#.o..T.P4.YLK. .P....F..
00:01:59.250692 IP 192.168.100.138.45396 > 35.232.111.17.80: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP/1.1
E...A.@.A.J..d.#.o..T.P4.YLK. .P.....GET / HTTP/1.1
Host: connectivity-check.ubuntu.com
Accept: */*
Connection: close

00:01:59.251412 IP 35.232.111.17.80 > 192.168.100.138.45396: Flags [.], ack 88, win 64240, length 0
E..(u.....#..o...d..P.TK. .4.Y.P...h.....
00:01:59.637841 IP 35.232.111.17.80 > 192.168.100.138.45396: Flags [FP.], seq 1:149, ack 88, win 64240, length 148: HTTP: HTTP/1.1 204 No Content
E...v.....#..o...d..P.TK. .4.Y.P...Q..HTTP/1.1 204 No Content
Date: Mon, 24 Jan 2022 18:31:59 GMT
Server: Apache/2.4.18 (Ubuntu)
X-NetworkManager-Status: online
Connection: close

00:01:59.638322 IP 192.168.100.138.45396 > 35.232.111.17.80: Flags [F.], seq 88, ack 150, win 64091, length 0
E..(A.@.A...d.#.o..T.P4.Y.K
.P..[F..
00:01:59.638951 IP 35.232.111.17.80 > 192.168.100.138.45396: Flags [.], ack 89, win 64239, length 0
E..(w.....#..o...d..P.TK
.4.Y.P...gy.....
00:02:03.845642 IP 192.168.100.138.34676 > 216.92.49.183.80: Flags [S], seq 3192748716, win 64240, options [mss 1460,sackOK,TS val 1150092012 ecr 0,nop,wscale 7], length 0
E..<..@.@.....d..1..t.P.Mz...../u.....
D.....
10 packets captured
10 packets received by filter
0 packets dropped by kernel
pesiug20cs445@sundeep:~/Desktop$

```

Step 5: To save packets to a file instead of displaying them on screen

```

pesiug20cs445@sundeep:~/Desktop$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
10 packets captured
28 packets received by filter
0 packets dropped by kernel
pesiug20cs445@sundeep:~/Desktop$

```



## Task 5: Perform Traceroute checks

### Step 1: Run the traceroute

```
pes1ug20cs445@sundeep:~/Desktop$ sudo traceroute www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1 _gateway (192.168.100.2)  1.749 ms  0.637 ms  0.204 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

### Step 2: Analyze destination address of google.com and no. of hops

Destination Address – 142.25067.228

Max number of hops – 30

### Step 3: To speed up the process, you can disable the mapping of IP addresses with hostnames

```
pes1ug20cs445@sundeep:~/Desktop$ sudo traceroute -n www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1 192.168.100.2  0.352 ms  0.231 ms  0.161 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

### Step 4: : The -I option is necessary so that the traceroute uses ICMP.

```
pes1ug20cs445@sundeep:~/Desktop$ sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1 _gateway (192.168.100.2) 0.682 ms 0.578 ms 0.481 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 bom07s24-in-f4.1e100.net (142.250.67.228) 34.345 ms 35.021 ms 39.275 ms
pes1ug20cs445@sundeep:~/Desktop$
```

Step 5: : By default, traceroute uses icmp (ping) packets. If you'd rather test a TCP connection to gather data more relevant to web server, you can use the -T flag

```
pes1ug20cs445@sundeep:~/Desktop$ sudo traceroute -T www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1 _gateway (192.168.100.2) 1.435 ms 0.397 ms 0.199 ms
 2 bom07s24-in-f4.1e100.net (142.250.67.228) 33.666 ms 37.041 ms 36.983 ms
pes1ug20cs445@sundeep:~/Desktop$
```

## Task 6: Explore an entire network for information (Nmap)

Step 1: You can scan a host using its host name or IP address, for instance.

```
pes1ug20cs445@sundeep:~/Desktop$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-25 00:18 IST
Nmap scan report for www.pes.edu (52.172.204.196)
Host is up (0.042s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 93.03 seconds
```

Step 2: Alternatively, use an IP address to scan.

```
pes1ug20cs445@sundeep:~/Desktop$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-25 00:22 IST
Nmap scan report for 163.53.78.128
Host is up (0.057s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 69.14 seconds
```

Step 3: Scan multiple IP address or subnet (IPv4)

```
pes1ug20cs445@sundeep:~/Desktop$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-25 00:24 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.09 seconds
pes1ug20cs445@sundeep:~/Desktop$
```

## Questions on above observations:

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

Answer - The Firefox browser used is running HTTP v1.1, and this can be seen in the request header which contains the method (GET) followed by the HTTP version. Similarly, the HTTP version of the web server is v1.1 and can be seen in the header of the HTTP response sent back to the browser.

HTTP Request:

```

  ▾ Hypertext Transfer Protocol
    ▸ GET /qatweb1.html HTTP/1.1\r\n

```

HTTP response:

```

  ▾ Hypertext Transfer Protocol
    ▸ HTTP/1.1 304 Not Modified\r\n

```

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

Answer - We can find the last modified time of the HTML file at the server by observing the Last-Modified field of the HTTP response object. The Last-Modified field stores a timestamp of the last modification time.

```
Last-Modified: Fri, 05 Feb 2021 22:45:48 GMT
Accept-Ranges: bytes
```

3. How to tell ping to exit after a specified number of ECHO\_REQUEST packets?

Answer - Ping continues to send ICMP packages until it receives an interrupt signal. To specify the number of ECHO\_REQUEST packages after which ping will exit, we can use the -c option followed by the number of packages.

Command: ping -c 10 [www.google.com](http://www.google.com)

```
pesiug20cs445@sundeep:~/Desktop$ ping -c 10 www.google.com
PING www.google.com (142.250.67.228) 56(84) bytes of data.
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=1 ttl=128 time=35.3 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=2 ttl=128 time=35.2 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=3 ttl=128 time=37.3 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=4 ttl=128 time=36.2 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=5 ttl=128 time=38.8 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=6 ttl=128 time=36.0 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=7 ttl=128 time=36.1 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=8 ttl=128 time=36.4 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=9 ttl=128 time=36.0 ms
64 bytes from bom07s24-in-f4.1e100.net (142.250.67.228): icmp_seq=10 ttl=128 time=37.6 ms

--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 35.235/36.503/38.752/1.028 ms
```

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

Answer: 1. We can obtain the remote host app and OS of the server by observing the Server files of the HTTP response object. The Server field stores the remote host app or server on which it is hosted and the OS too.

```
HTTP/1.1 304 Not Modified\r\n
Date: Mon, 24 Jan 2022 19:27:19 GMT\r\n
Server: Apache\r\n
Last-Modified: Fri, 05 Feb 2021 22:45:48 GMT\r\n
```

2. We can use nmap to find the OS too. It will scan the network to find information about the remote host apps and OS.

```
pesiug20cs445@sundeep:~/Desktop$ sudo nmap -O -v www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-25 00:51 IST
Initiating Ping Scan at 00:51
Scanning www.google.com (142.250.67.228) [4 ports]
Completed Ping Scan at 00:51, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:51
Completed Parallel DNS resolution of 1 host. at 00:51, 0.03s elapsed
Initiating SYN Stealth Scan at 00:51
Scanning www.google.com (142.250.67.228) [1000 ports]
Discovered open port 443/tcp on 142.250.67.228
Discovered open port 80/tcp on 142.250.67.228
Increasing send delay for 142.250.67.228 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 142.250.67.228 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed SYN Stealth Scan at 00:52, 46.21s elapsed (1000 total ports)
Initiating OS detection (try #1) against www.google.com (142.250.67.228)
Nmap scan report for www.google.com (142.250.67.228)
Host is up (0.021s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:814::2004
rDNS record for 142.250.67.228: bom07s24-in-f4.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7::sp1
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
TCP Sequence Prediction: Difficulty=255 (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 48.44 seconds
Raw packets sent: 2067 (92.810KB) | Rcvd: 1404 (56.867KB)
```