

Exercise 1 – Basic network stuff

Difficulty: **Easy**

Use the `arp` command and paste the output from the arp table on your system:

```
C:\Users\Acer>arp -a

Interface: 192.168.0.14 --- 0xe
    Internet Address      Physical Address      Type
    192.168.0.1           0c-b9-37-27-d3-30    dynamic
    192.168.0.13          ce-cf-df-05-67-ca    dynamic
    192.168.0.15          3c-a0-67-8e-75-ed    dynamic
    192.168.0.255         ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 172.23.112.1 --- 0x2a
    Internet Address      Physical Address      Type
    172.23.123.81         00-15-5d-b1-13-fe    dynamic
    172.23.127.255        ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static

C:\Users\Acer>
```

Use the **route** command and paste the output from the routing table on your system:

```
C:\Users\Acer>route print
=====
Interface List
16...b4 a9 fc 48 09 56 .....Realtek PCIe GbE Family Controller
15...12 63 c8 bb aa d9 .....Microsoft Wi-Fi Direct Virtual Adapter
17...22 63 c8 bb aa d9 .....Microsoft Wi-Fi Direct Virtual Adapter #2
14...10 63 c8 bb aa d9 .....Qualcomm Atheros QCA9377 Wireless Network Adapter
1.....Software Loopback Interface 1
42...00 15 5d 96 c8 a4 .....Hyper-V Virtual Ethernet Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface         Metric
0.0.0.0                    0.0.0.0          192.168.0.1       192.168.0.14      55
127.0.0.0                  255.0.0.0        On-link           127.0.0.1         331
127.0.0.1                  255.255.255.255  On-link           127.0.0.1         331
127.255.255.255            255.255.255.255  On-link           127.0.0.1         331
172.23.112.0               255.255.240.0    On-link           172.23.112.1      5256
172.23.112.1               255.255.255.255  On-link           172.23.112.1      5256
172.23.127.255             255.255.255.255  On-link           172.23.112.1      5256
192.168.0.0                255.255.255.0    On-link           192.168.0.14      311
192.168.0.14               255.255.255.255  On-link           192.168.0.14      311
192.168.0.255              255.255.255.255  On-link           192.168.0.14      311
224.0.0.0                  240.0.0.0        On-link           127.0.0.1         331
224.0.0.0                  240.0.0.0        On-link           192.168.0.14      311
224.0.0.0                  240.0.0.0        On-link           172.23.112.1      5256
255.255.255.255            255.255.255.255  On-link           127.0.0.1         331
255.255.255.255            255.255.255.255  On-link           192.168.0.14      311
255.255.255.255            255.255.255.255  On-link           172.23.112.1      5256
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1    331 ::1/128                      On-link
14   311 fe80::/64                    On-link
42   5256 fe80::/64                    On-link
14   311 fe80::b44c:619c:3325:5dc5/128
                                         On-link
42   5256 fe80::ed38:8738:f6e6:5e8a/128
                                         On-link
1    331 ff00::/8                     On-link
```

Use the **tracert** command on your system and observe the hops to Google's DNS, 8.8.8.8. Paste the full output from the command below showing all the hops from your system to 8.8.8.8.

```
C:\Users\Acer>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  0  7 ms   1 ms   1 ms  192.168.0.1
  1  10 ms   9 ms   8 ms  10.181.224.1
  2  *       *       *     Request timed out.
  3  *       *       *     Request timed out.
  4  *       *       *     Request timed out.
  5  *       *       *     Request timed out.
  6  *       *       *     Request timed out.
  7  *       *       *     Request timed out.
  8  10 ms   13 ms   9 ms  ctel-78-157-16-209.cabletel.com.mk [78.157.16.209]
  9  31 ms   31 ms   29 ms  195.3.114.153
 10  28 ms   29 ms   30 ms  lg22-9070.as8447.a1.net [195.3.64.57]
 11  *       *       *     Request timed out.
 12  33 ms   35 ms   31 ms  lg59-9071.as8447.a1.net [80.120.167.46]
 13  35 ms   34 ms   32 ms  172.253.51.153
 14  36 ms   36 ms   37 ms  142.251.65.227
 15  33 ms   32 ms   32 ms  dns.google [8.8.8.8]

Trace complete.

C:\Users\Acer>
```

Why would you need to use the ping command?

Answer:

```
C:\Users\Acer>ping -t google.com

Pinging google.com [142.250.201.206] with 32 bytes of data:
Reply from 142.250.201.206: bytes=32 time=32ms TTL=109
Reply from 142.250.201.206: bytes=32 time=31ms TTL=109
Reply from 142.250.201.206: bytes=32 time=31ms TTL=109
Reply from 142.250.201.206: bytes=32 time=33ms TTL=109
Reply from 142.250.201.206: bytes=32 time=31ms TTL=109
Reply from 142.250.201.206: bytes=32 time=30ms TTL=109
Reply from 142.250.201.206: bytes=32 time=31ms TTL=109
Reply from 142.250.201.206: bytes=32 time=31ms TTL=109

Ping statistics for 142.250.201.206:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 33ms, Average = 31ms
Control-C
^C
C:\Users\Acer>
```

Write down the TCP/UDP ports of the most commonly used services bellow in the form of TCP[PORT] or UDP[PORT].


As an example, the first two answers have been filled in:

- HTTP – TCP80
- SNMP – UDP161
- HTTPS – Port 443
- DNS client – Port range 1024-65535
- DNS zone transfer – TCP port 53
- SMTP – TCP port 25
- SSH – TCP port 22
- FTP – TCP port 21
- Telnet – TCP port 23
- MSSQL – TCP port 1433
- MySQL -TCP port 3306
- PostgreSQL – TCP port 5432
- RDP (Remote Desktop Protocol) – TCP port 3389
- NTP – TCP 123
- NFS – TCP port 2049

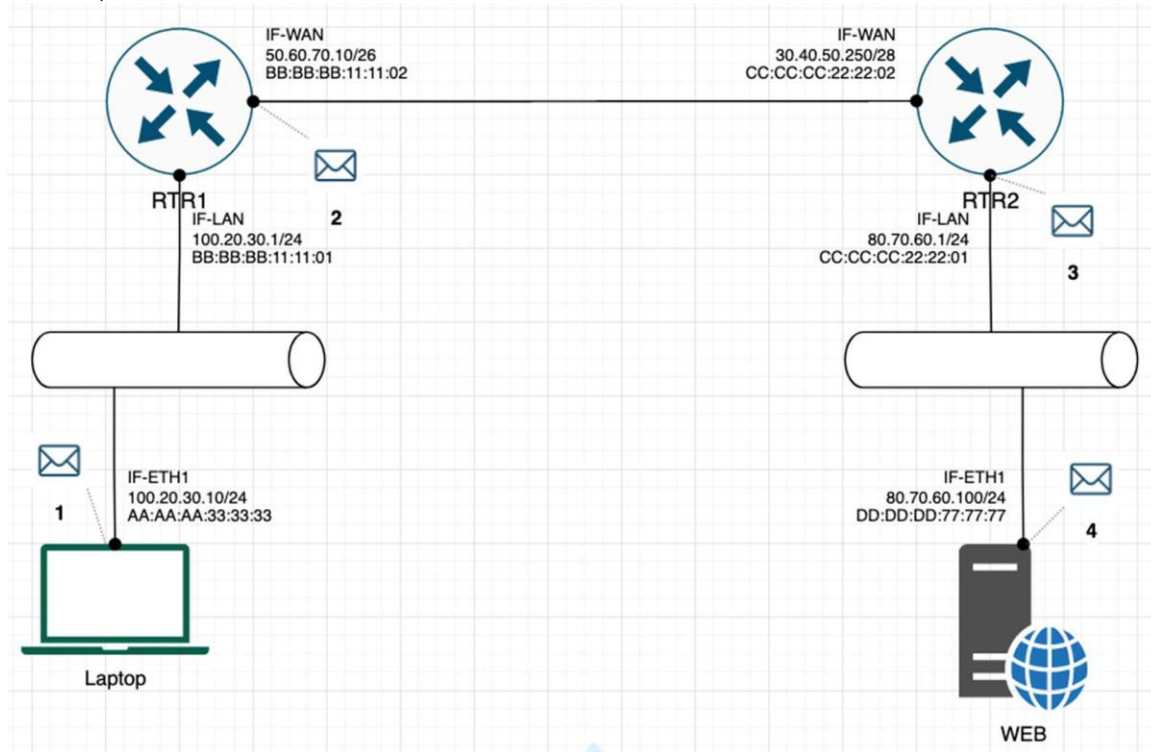
Exercise 2 – TCP/IP Basics

Difficulty: **Medium**

Refer to the exhibit and answer the questions below.

The letter symbol , represents the IP packet as it travels across the network. In the example shown, the laptop attempts to communicate with the web server in question. During its travel the packet will be forwarded across the network nodes and will eventually end up across six network interfaces before it reaches the web server. Each

packet as part of the TCP/IP Stack contains fields for the source and destination MAC Address, IP Address and the TCP/UDP Port.



For each of the packet locations shown, 1 to 4 write down the source and destination MAC addresses of the packet as it travels across the network interfaces.

- The laptop initiates communication with the web server and prepares a packet. What would the packet look like at this stage?
 - SRC IP: Laptop's IP
 - DST IP : Web server's IP address
 - SRC MAC : Laptop's MAC address
 - DST MAC : MAC address of the first router interface facing the laptop
- RTR1 receives the packet on its IF-LAN interface, prepares it accordingly and forwards it out its IF-WAN. What would the packet look like at this stage?
 - SRC IP : Laptop's IP address
 - DST IP : Web server's IP address
 - SRC MAC : MAC address of the first router's interface facing laptop (LAN)
 - DST MAC : MAC address of the second router's interface facing the first router
- RTR2 receives the packet on its IF-WAN interface, prepares it accordingly and forwards it out via IF-LAN. What would the packet look like at this stage?
 - SRC IP: Laptop's IP address
 - DST IP : Web server's IP address
 - SRC MAC: MAC address of the second router's interface facing the first router
 - DST MAC : MAC address of the second router's interface facing the web server

4. The web server receives the packet and prepares a response packet back. What would the packet look like at this stage?
- SRC IP : Web server's IP address
 - DST IP : Laptop's IP address
 - SRC MAC : Web servers MAC address
 - DST MAC : MAC address of the second router's interface facing the web server

Since we are talking about web traffic (www) in the example, which transport layer protocol will most probably be used?

- ☐ **TCP**
- ☐ UDP

If we do a traffic analysis with a network packet monitoring tool like WireShark, what can we expect to see for the source and destination ports when the laptop sends the packet?

- SRC PORT: Port from 1024 and above
- DST PORT: HTTPS Port 443 (it depend of the service)

Similarly, and vice versa, what can we expect to see as destination ports when the Web server sends a response packet back?

- SRC PORT: HTTPS 443 (it depend of the service)
- DST PORT: Port from 1024 and above

How many broadcast domains are there in the exhibit shown? 2

Exercise 3 – Traffic analysis and identifying the OSI layers of the network packets

Difficulty: **Hard**

Prerequisite:

Search online and get familiar with the TCP's three-way handshake. Learn how to capture the three way handshake using Wireshark.

Install Wireshark on your computer and use it to capture traffic against a website or a server or your choice. It is recommended that you capture traffic against a simple website. Name and the IP address of the website you plan to capture traffic:

Analyze the TCP's three-way handshake and using screenshots from the Wireshark window answer the questions below:

1. What is the source IP (of the initiating host):

2. What is the destination IP? (target website):

Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:

The top screenshot shows a Wireshark packet capture window. The packet list on the left shows a SYN packet (No. 14) with source 192.168.0.14 and destination 40.101.69.210. The packet details pane on the right shows the Ethernet II section, indicating the source and destination MAC addresses and the interface used.

The bottom screenshot shows the same packet capture window, but with the packet details pane expanded to show the Internet Protocol section. The source IP is 192.168.0.14 and the destination IP is 40.101.69.210. The packet details pane also shows the Ethernet II section, indicating the source and destination MAC addresses and the interface used.

Identify the Network Layer 3 section of the SYN/ACK packet and paste a screenshot from it:

Wi-Fi (tcp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.14	40.101.69.210	TCP	55	51819 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
2	0.034363	40.101.69.210	192.168.0.14	TCP	66	443 → 51819 [ACK] Seq=1 Ack=2 Win=16380 Len=0 SLE=1 SRE=2
3	0.110258	192.168.0.14	23.102.0.171	TLSv1.2	112	Application Data
4	0.266721	23.102.0.171	192.168.0.14	TLSv1.2	101	Application Data
5	0.313044	192.168.0.14	23.102.0.171	TCP	54	61263 → 443 [ACK] Seq=59 Ack=48 Win=515 Len=0
6	0.852557	192.168.0.14	52.149.21.60	TCP	1494	50452 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1440 [TCP segment of a reassembled PDU]
7	0.852557	192.168.0.14	52.149.21.60	TCP	1494	50452 → 443 [ACK] Seq=1441 Ack=1 Win=516 Len=1440 [TCP segment of a reassembled PDU]
8	0.852557	192.168.0.14	52.149.21.60	TLSv1.2	973	Application Data
9	0.852919	192.168.0.14	52.149.21.60	TLSv1.2	98	Application Data
10	1.062944	52.149.21.60	192.168.0.14	TCP	60	443 → 50452 [ACK] Seq=1 Ack=2881 Win=2053 Len=0
11	1.065399	52.149.21.60	192.168.0.14	TCP	60	443 → 50452 [ACK] Seq=1 Ack=3844 Win=2049 Len=0
12	1.065399	52.149.21.60	192.168.0.14	TLSv1.2	375	Application Data
13	1.106960	192.168.0.14	52.149.21.60	TCP	54	50452 → 443 [ACK] Seq=3844 Ack=322 Win=514 Len=0
14	3.294753	192.168.0.14	142.250.201.195	TCP	66	51918 → 443 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15	3.330364	142.250.201.195	192.168.0.14	TCP	66	443 → 51918 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
16	3.330453	192.168.0.14	142.250.201.195	TCP	54	51918 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
17	3.331080	192.168.0.14	142.250.201.195	TLSv1.3	571	Client Hello

Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D6623905-...} Ethernet II, Src: LiteonTe.bb:aa:d9 (10:63:c8:bb:aa:d9), Dst: LiteonTe.bb:aa:d9 (10:63:c8:bb:aa:d9)

Internet Protocol Version 4, Src: 142.250.201.195, Dst: 192.168.0.14

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x0000 (0)
 010. = Flags: 0x2, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 115
 Protocol: TCP (6)
 Header checksum: 0xeeef [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 142.250.201.195
 Destination Address: 192.168.0.14

Transmission Control Protocol, Src Port: 443, Dst Port: 51918, Seq: 0, Ack: 1, Len: 0

Identify the Transport Layer 4 section of the ACK packet and paste a screenshot from it bellow:

Wi-Fi (tcp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
10	1.062944	52.149.21.60	192.168.0.14	TCP	60	443 → 50452 [ACK] Seq=1 Ack=2881 Win=2053 Len=0
11	1.065399	52.149.21.60	192.168.0.14	TCP	60	443 → 50452 [ACK] Seq=1 Ack=3844 Win=2049 Len=0
12	1.065399	52.149.21.60	192.168.0.14	TLSv1.2	375	Application Data
13	1.106960	192.168.0.14	52.149.21.60	TCP	54	50452 → 443 [ACK] Seq=3844 Ack=322 Win=514 Len=0
14	3.294753	192.168.0.14	142.250.201.195	TCP	66	51918 → 443 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15	3.330364	142.250.201.195	192.168.0.14	TCP	66	443 → 51918 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
16	3.330453	192.168.0.14	142.250.201.195	TCP	54	51918 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
17	3.331080	192.168.0.14	142.250.201.195	TLSv1.3	571	Client Hello

Frame 16: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{D6623905-...} Ethernet II, Src: LiteonTe.bb:aa:d9 (10:63:c8:bb:aa:d9), Dst: LiteonTe.bb:aa:d9 (10:63:c8:bb:aa:d9)

Internet Protocol Version 4, Src: 192.168.0.14, Dst: 142.250.201.195

Transmission Control Protocol, Src Port: 51918, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

Source Port: 51918
 Destination Port: 443
 [Stream index: 3]
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 398895738
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 29497981
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
 Window: 512
 [Calculated window size: 131072]
 [Window size scaling factor: 256]
 Checksum: 0xa956 (unverified)
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > [Timestamps]
 > [SEQ/ACK analysis]

Look closely at the L2 section of the three-way handshake packet details. Each of them shows the source and destination MAC address of the packets.

Who is the owner of the destination MAC address of the SYN packet?

lookup MAC address

SELECT LOOKUP TYPE: ☒ LOOKUP MAC ☐ LOOKUP VENDOR

example: 00:0B:14

Results for MAC address 0C:B9:37:27:D3:30

Found 1 result

MAC Address	0C:B9:37:27:D3:30
Vendor	Ubee Interactive Co., Limited
Address	Flat/RM 1202, 12/F, AT Tower North Point Hong Kong 180 HK
Block Size	MA-L
Block Range	0C:B9:37:00:00:00 - 0C:B9:37:FF:FF:FF

Exercise 4 – Hacking mockup (for Bonus points)

Difficulty: **Very hard**

Use Wireshark to capture the packet's application layer data and discover the implications of using unencrypted communication over a network.

It is recommended that you use your own Linux Virtual Machine on your system on which you need to configure a telnet server.

From your own system try to login with a Telnet on the target VM all while capturing the traffic with a Wireshark. As a proof of competition for this exercise paste in bellow a screenshot of the application layer data containing visible username and password.