

# Exercise 1 - Basic Networking

- **arp -a**

Interface: 192.168.56.1 --- 0x10

Internet Address	Physical Address	Type
192.168.56.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	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: 192.168.1.119 --- 0x21

Internet Address	Physical Address	Type
192.168.1.1	00-5f-67-55-ba-30	dynamic
192.168.1.7	6a-2c-c5-06-fd-e1	dynamic
192.168.1.127	00-d8-61-fc-1c-44	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	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: 172.22.240.1 --- 0x40

Internet Address	Physical Address	Type
172.22.242.27	00-15-5d-24-73-63	dynamic
172.22.255.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
239.255.255.250	01-00-5e-7f-ff-fa	static

- **route PRINT**

## IPv4 Route Table

```
=====
```

Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.119	25
	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
	172.22.240.0	255.255.240.0	On-link	172.22.240.1	271
	172.22.240.1	255.255.255.255	On-link	172.22.240.1	271
172.22.255.255	255.255.255.255		On-link	172.22.240.1	271
	192.168.1.0	255.255.255.0	On-link	192.168.1.119	281
192.168.1.119	255.255.255.255		On-link	192.168.1.119	281
192.168.1.255	255.255.255.255		On-link	192.168.1.119	281
	192.168.56.0	255.255.255.0	On-link	192.168.56.1	281
	192.168.56.1	255.255.255.255	On-link	192.168.56.1	281
192.168.56.255	255.255.255.255		On-link	192.168.56.1	281
	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	192.168.56.1	281
	224.0.0.0	240.0.0.0	On-link	192.168.1.119	281
	224.0.0.0	240.0.0.0	On-link	172.22.240.1	271
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	192.168.56.1	281
255.255.255.255	255.255.255.255		On-link	192.168.1.119	281
255.255.255.255	255.255.255.255		On-link	172.22.240.1	271

```
=====
```

- google dns server

tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]

over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	1 ms	1 ms	<1 ms	10.110.0.2
3	*	*	*	Request timed out.
4	*	*	*	Request timed out.
5	9 ms	9 ms	9 ms	212-39-66-222.ip.btc-net.bg [212.39.66.222]
6	10 ms	10 ms	10 ms	216.239.62.49
7	9 ms	11 ms	9 ms	209.85.254.243
8	9 ms	8 ms	8 ms	dns.google [8.8.8.8]

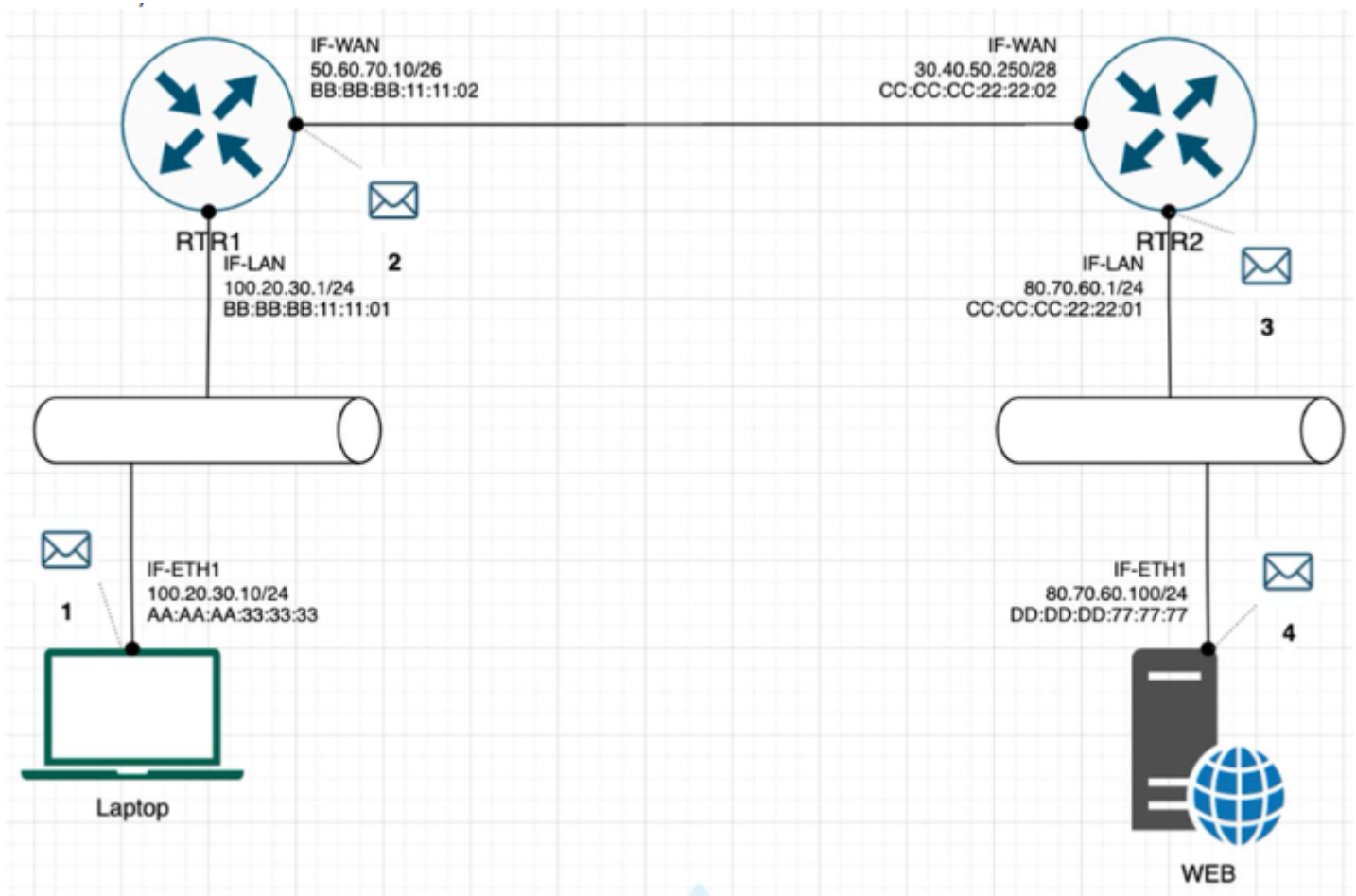
- **Why would you need to use the ping command ?**

Checking if the host is alive, latency, troubleshooting connection, PoD(ping of death)

Protocol	TCP	UDP	PORT
HTTP	x		80
SNMP		x	161
HTTPS	x		443
DNS Client		x	53
DNS Zone Transfer	x		53
SMTP	x		587
SSH	X		22
TELNET	x		23
FTP	x		20,21
MYSQL	x		3306
MSSQL	x		1433
PostresSQL	x		5432
RDP	x		3389
NTP		x	123
NFS	x		2049

## Exercise 2 – TCP/IP Basics:

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.**

1. The laptop initiates communication with the web server and prepares a packet. What would the packet look like at this stage?
  - SRC IP 100.20.30.10
  - DST IP 80.70.60.100
  - SRC MAC AA:AA:AA:33:33:33
  - DST MAC BB:BB:BB:11:11:01

2. 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 100.20.30.10
  - DST IP 80.70.60.100
  - SRC MAC BB:BB:BB:11:11:02
  - DST MAC CC:CC:CC:22:22:02
3. 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 100.20.30.10
  - DST IP 80.70.60.100
  - SRC MAC CC:CC:CC:22:22:01
  - DST MAC DD:DD:DD:77:77:77
4. The web server receives the packet and prepares a response packet back. What would the packet look like at this stage?
  - SRC IP 80.70.60.100
  - DST IP 100.20.30.10
  - SRC MAC DD:DD:DD:77:77:77
  - DST MAC CC:CC:CC:22:22:01

**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: ephemeral port
- DST PORT: well-know port

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

- SRC PORT: well-know port
- DST PORT: ephemeral port

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

- 4 broadcast domains

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

target site	IP adress
www.scalefocus.academy	34.117.168.233

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):

Time	Source	Destination	Protocol
4.103608	192.168.1.119	34.117.168.233	TCP

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

▼ Frame 76: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF\_{9ADD1A22-7774-412A-9376-C4D352E6CA30}, Section number: 1

➤ Interface id: 0 (\Device\NPF\_{9ADD1A22-7774-412A-9376-C4D352E6CA30})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 15, 2023 07:21:39.746572000 FLE Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1678857699.746572000 seconds

[Time delta from previous captured frame: 0.000311000 seconds]

[Time delta from previous displayed frame: 0.338210000 seconds]

[Time since reference or first frame: 4.103608000 seconds]

Frame Number: 76

Frame Length: 70 bytes (560 bits)

Capture Length: 70 bytes (560 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: TCP SYN/FIN]

[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]

▼ Ethernet II, Src: ASUSTekC\_86:bd:16 (60:45:cb:86:bd:16), Dst: TP-Link\_55:ba:30 (00:5f:67:55:ba:30)

▼ Destination: TP-Link\_55:ba:30 (00:5f:67:55:ba:30)

Address: TP-Link\_55:ba:30 (00:5f:67:55:ba:30)

.... 0. .... = LG bit: Globally unique address (factory default)

.... 0. .... = IG bit: Individual address (unicast)

▼ Source: ASUSTekC\_86:bd:16 (60:45:cb:86:bd:16)

Address: ASUSTekC\_86:bd:16 (60:45:cb:86:bd:16)

.... 0. .... = LG bit: Globally unique address (factory default)

.... 0. .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

No.	Time	Source	Destination	Protocol	Length	Info
76	4.103608	192.168.1.119	34.117.168.233	TCP	70	[53807 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM

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

> Frame 85: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF\_{9ADD1A22-7774-412A-9376-C4D352E6CA30},

> Ethernet II, Src: TP-Link\_55:ba:30 (00:5f:67:55:ba:30), Dst: ASUSTekC\_86:bd:16 (60:45:cb:86:bd:16)

> Internet Protocol Version 4, Src: 34.117.168.233, Dst: 192.168.1.119

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 56

Identification: 0x0000 (0)

> 010. .... = Flags: 0x2, Don't fragment

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 122

Protocol: TCP (6)

Header Checksum: 0x7342 [validation disabled]

[Header checksum status: Unverified]

Source Address: 34.117.168.233

Destination Address: 192.168.1.119

> Transmission Control Protocol, Src Port: 443, Dst Port: 53807, Seq: 0, Ack: 1, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
85	4.118077	34.117.168.233	192.168.1.119	TCP	70	443 → 53807 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS

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

Transmission Control Protocol, Src Port: 53807, Dst Port: 443, Seq: 1, Ack: 1, Len: 0						
Source Port: 53807						
Destination Port: 443						
[Stream index: 10]						
[Conversation completeness: Incomplete, DATA (15)]						
[TCP Segment Len: 0]						
Sequence Number: 1 (relative sequence number)						
Sequence Number (raw): 3384920320						
[Next Sequence Number: 1 (relative sequence number)]						
Acknowledgment Number: 1 (relative ack number)						
Acknowledgment number (raw): 400410483						
1000 .... = Header Length: 32 bytes (8)						
Flags: 0x010 (ACK)						
000. .... = Reserved: Not set						
...0 .... = Accurate ECN: Not set						
.... 0... = Congestion Window Reduced: Not set						
.... .0.. = ECN-Echo: Not set						
.... ..0. = Urgent: Not set						
.... ...1 = Acknowledgment: Set						
.... .... 0... = Push: Not set						
.... .... .0.. = Reset: Not set						
.... .... ..0. = Syn: Not set						
.... .... ...0 = Fin: Not set						
[TCP Flags: .....A.....]						
Window: 64240						
[Calculated window size: 64240]						
[Window size scaling factor: -2 (no window scaling used)]						
Checksum: 0x143d [unverified]						
[Checksum Status: Unverified]						
Urgent Pointer: 0						
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
> [Timestamps]						
SEQ/ACK analysis						
<a href="#">[This is an ACK to the segment in frame: 85]</a>						
[The RTT to ACK the segment was: 0.000210000 seconds]						
[iRTT: 0.014679000 seconds]						

No.	Time	Source	Destination	Protocol	Length	Info
86	4.118287	192.168.1.119	34.117.168.233	TCP	66	53807 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSval=161992

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

Owner is the default gateway

## Exercise 4 – Hacking mockup (for Bonus points)

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.



Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 6

No.	Time	Source	Destination	Protocol	Length	Info
252	27.708345	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
254	27.708657	192.168.1.119	192.168.1.119	TCP	183	[TCP ...]
255	27.754099	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
256	27.754174	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
262	28.938770	192.168.1.119	192.168.1.119	TCP	67	[TCP ...]
264	28.982194	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
266	28.982936	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
268	29.073556	192.168.1.119	192.168.1.119	TCP	67	[TCP ...]
269	29.124333	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
270	29.124702	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
272	29.214016	192.168.1.119	192.168.1.119	TCP	67	[TCP ...]
273	29.266609	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
274	29.266698	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
277	29.617398	192.168.1.119	192.168.1.119	TCP	68	[TCP ...]
278	29.659256	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
279	29.659327	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
281	29.673140	192.168.1.119	192.168.1.119	TCP	634	[TCP ...]
282	29.720525	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
283	29.720777	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
285	29.721080	192.168.1.119	192.168.1.119	TCP	79	[TCP ...]
286	29.767134	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
287	29.767266	192.168.1.119	192.168.1.119	TCP	66	[TCP ...]
99	15.376930	192.168.1.119	192.168.1.119	TELNET	206	Telnet ...
104	15.417957	192.168.1.119	192.168.1.119	TELNET	78	Telnet ...
117	18.390894	192.168.1.119	192.168.1.119	TELNET	67	Telnet ...

> Frame 179: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface  
 > Ethernet II, Src: ASUSTekC\_86:bd:16 (60:45:cb:86:bd:16), Dst: TP-Link\_55:ba:30  
 > Internet Protocol Version 4, Src: 192.168.1.119, Dst: 192.168.1.119  
 > 0100 .... = Version: 4  
 > .... 0101 = Header Length: 20 bytes (5)  
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 > Total Length: 53  
 > Identification: 0xb961 (47457)  
 > 010. .... = Flags: 0x2, Don't fragment  
 > ...0 0000 0000 0000 = Fragment Offset: 0  
 > Time to Live: 128  
 > Protocol: TCP (6)  
 > Header Checksum: 0xbd22 [validation disabled]  
 > [Header checksum status: Unverified]  
 > Source Address: 192.168.1.119  
 > Destination Address: 192.168.1.119  
 > Transmission Control Protocol, Src Port: 61218, Dst Port: 23, Seq: 8, Ack: 160,  
 > Telnet

Wireshark - Follow TCP Stream (tcp.stream eq 6) - Ethernet

Hadi Kiamarsi Telnet Server Version 3.0.1

E-Mail : hadikiamarsi@gmail.com

WebPage : <http://sourceforge.net/projects/hk-telnet-server>

Username: ZZ33RR00CC0000LL

Password: 1\*3\*3\*7\*

[ USERNAME = Z3R0C00L ] YOUR IP ADDRESS : 192.168.1.119  
 Welcome to Hadi Kiamarsi TELNET Server.

TELNET # C:\>dir  
 Volume in drive C has no label.  
 Volume Serial Number is A412-DA95

Directory of C:\

Date/Time	File Name	Size	Attributes
28/06/2022 09:31	<DIR>		edb
13/03/2023 10:22	<DIR>		Intel
06/03/2023 07:29	<DIR>		Program Files
27/01/2023 08:36	<DIR>		Program Files (x86)
18/02/2023 17:26	<DIR>		Python311
28/06/2022 09:37	<DIR>		Users
13/03/2023 08:10	<DIR>		Windows
17/02/2023 20:39	<DIR>		XboxGames
	0 File(s)	0 bytes	
	8 Dir(s)	18,286,444,544 bytes free	

TELNET # C:\>

Windows is a bit finicky with loopbacks.

Solution I used is adding a route => my machine > router > my machine. This information is in the loopback section of wireshark