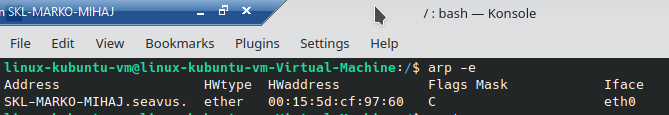
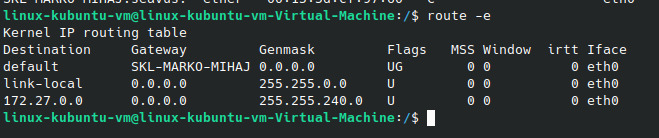
# Exercise 1 – Basic network stuff

Difficulty: **Easy**

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

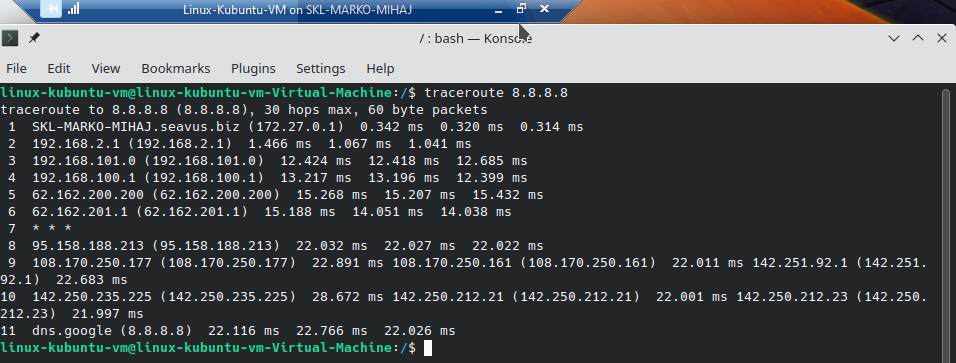


Use the route command and paste the output from the routing table on your system:



Use the traceroute command on your system and observe the hops to Google’s DNS,

* + - 1. Paste the full output from the command bellow showing all the hops from your system to 8.8.8.8.



## Why would you need to use the ping command?

Answer: The Ping command is used to see if we have a “clear path” – successful connection to another internet enabled device. We send the “ping” and see if the destinaniton is reachable. Note that devices can be set to ignore ping requests.

## 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 - UDP 161
        + HTTPS - TCP 443
        + DNS - UDP 53 - Client
        + DNS - TCP 53 - Zone transfer
        + SMTP - TCP 25
        + SSH - TCP 22
        + FTP - TCP 21
        + Telnet - TCP 23
        + MSSQL - TCP 1433
        + MySQL - TCP 3306
        + PostreSQL - TCP 5432
        + RDP - (Remote Desktop Protocol) TCP 3389
        + NTP - UDP 123
        + NFS - Uses port 2049 TCP or UDP port 111

# Exercise 2 – TCP/IP Basics

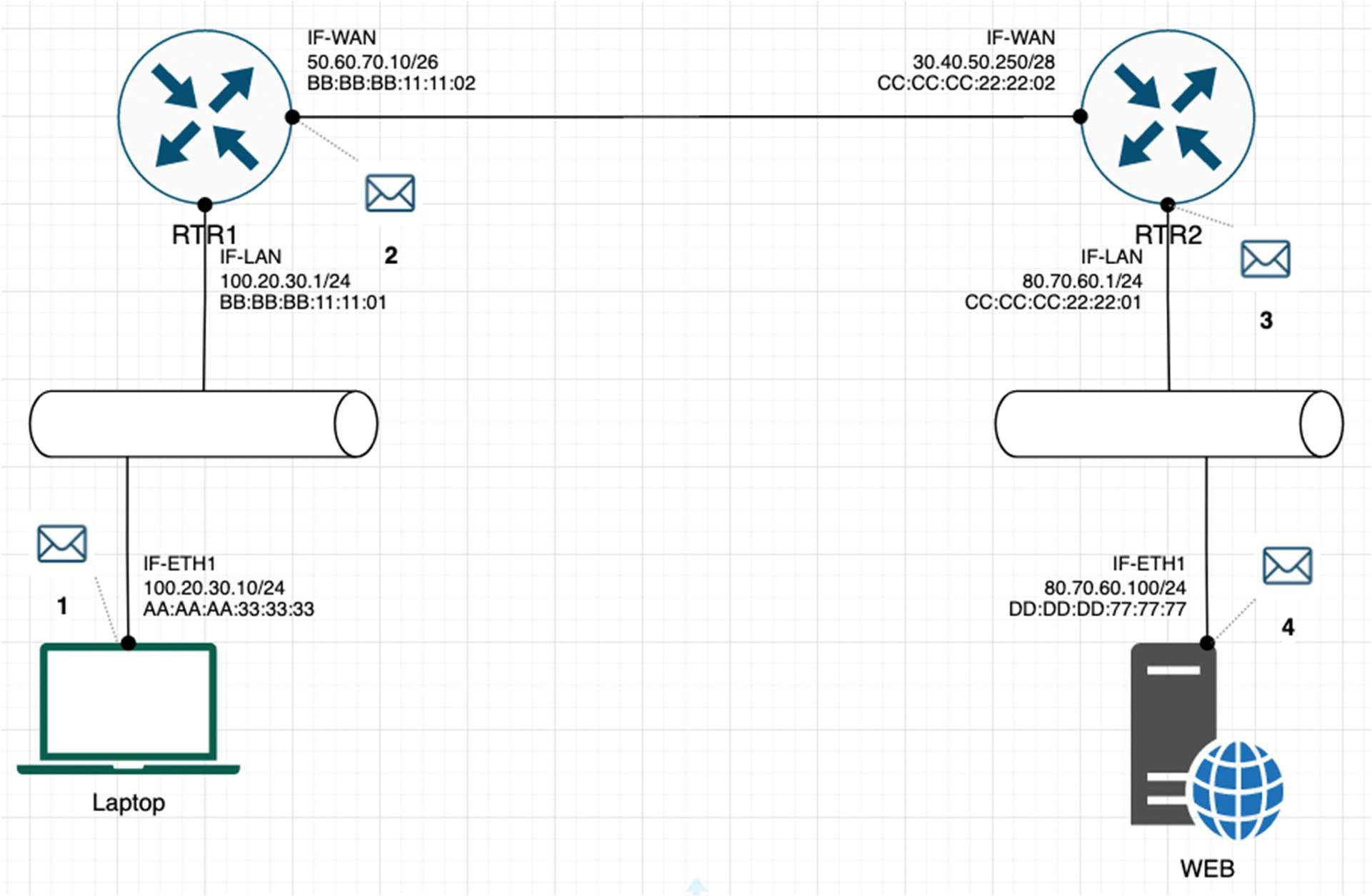
Difficulty: **Medium**

## 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.

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 – Will be used most likely. Except for live streams where where the constant flow of packets is more important than integrity. Other usecases as well for UDP but its not web traffic but traffic directly from applications on other ports.
* 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?

## Lets give a specific example. In my case I was pinging (194.149.144.75) feit.ukim.edumk

* + - * + SRC PORT: Random port from the unregistered port range on my Laptop – in this case **43524**
        + DST PORT: The port through which the request is accepted, the open port for type of request. In this case the webpage is http: port 80

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

* + - * + SRC PORT: Source port is the same as the destination port from before – port 80, so my Laptop when it receives the information back from the sent request it accepts it only if the data comes back from the same ip/port as it was sent to. This is done so the request is properly rooted back to the same Computer(ip), program/service (port) that initiated the request.
        + DST PORT: Destination port is the same as the source port from before – port 43524 which is still open waiting for the response from the request that was sent. When the response is received or after timeout period if the port is not needed anymore it is closed by the program.

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

There are two broadcast domains because the routers do not forward broadcasts from one of their interfaces to another so the bottom parts if the network inside the LAN are separate broadcast domains.

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

Difficulty: **Hard**

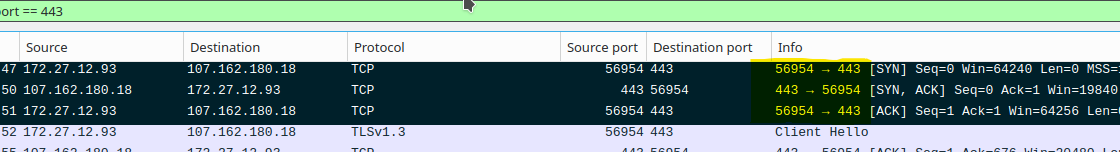
## Prerequisite:

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

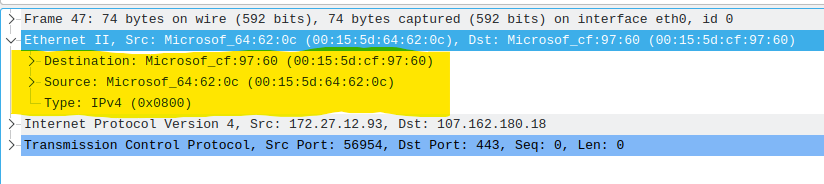
Install Wireshark on your computer and use it to capture traffic against a website or a server or your choice. It is recommended that you capture traffic against a simple website. Name and the IP address of the website you plan to capture traffic: **atmarko.cloud** (**107.162.180.18) – dynamic ip (changes)**

## Analyze the TCP’s three-way handshake and using screenshots from the Wireshark window answer the questions bellow:

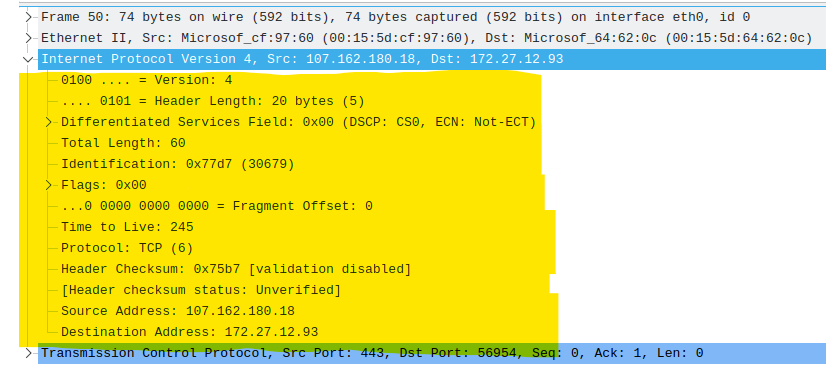
1. What is the source IP (of the initiating host): The Source ip is my local VM’s ip address assigned from my Windows host (172.27.12.93)
2. What is the destination IP? (target website): 107.162.180.18



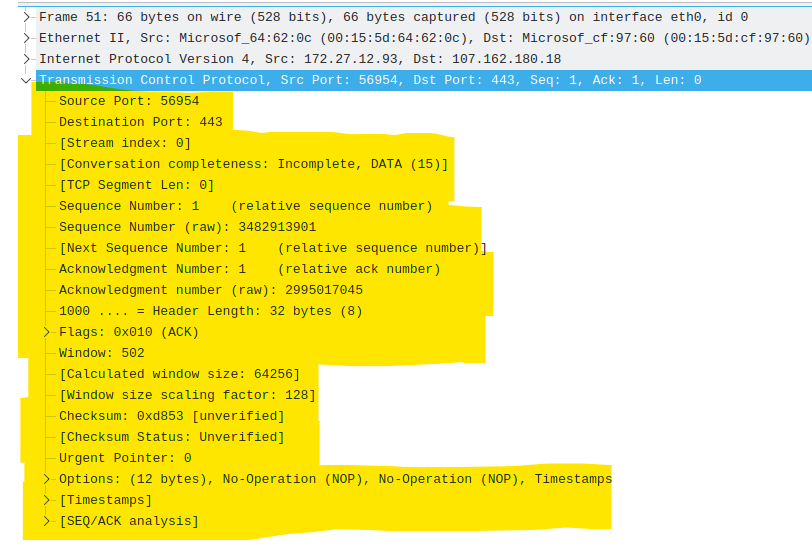
## Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:



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



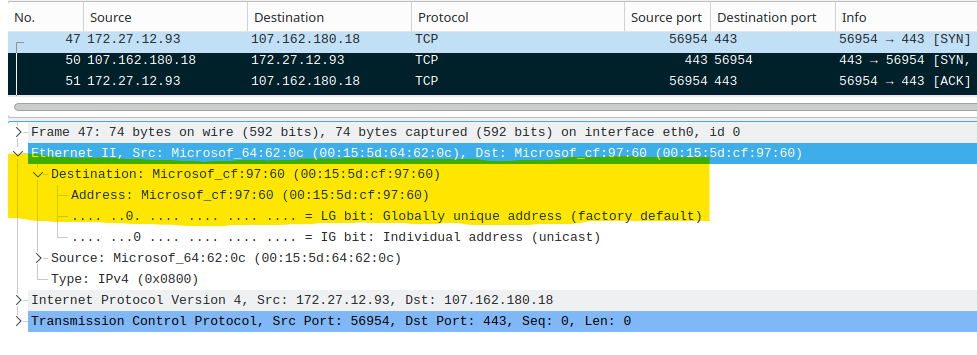
## Identify the Transport Layer 4 section of the ACK packet and paste a screenshot from it bellow:



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?**

In my specific case it is Microsoft.

****

# 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 confiture 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.



