Exercise 1 – Basic network stuff

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

A picture containing calendar

Description automatically generated

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

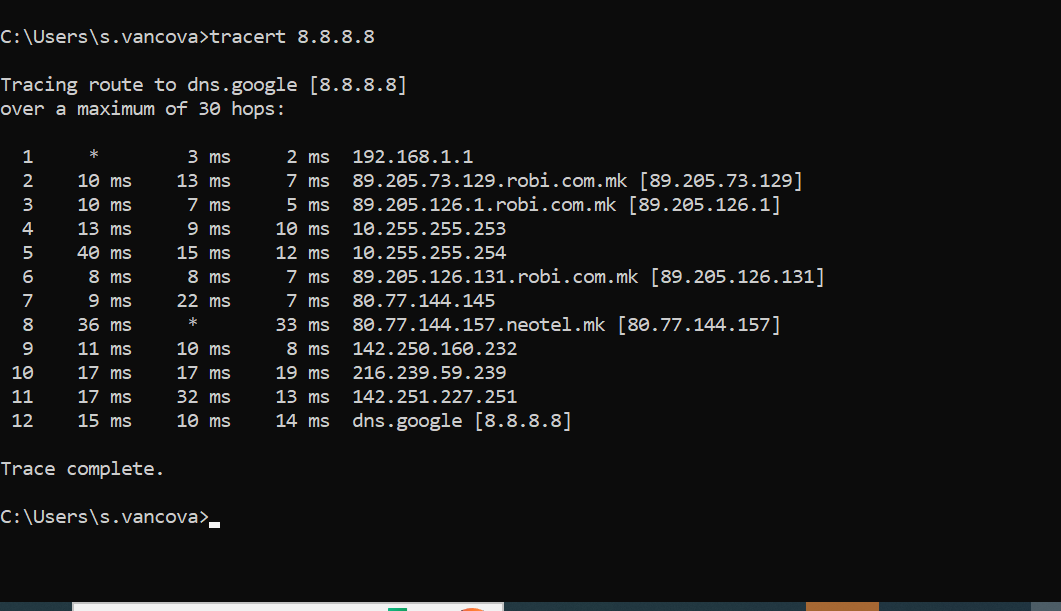
Graphical user interface, text

Description automatically generated

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

8.8.8.8. Paste the full output from the command bellow showing all the hops from your

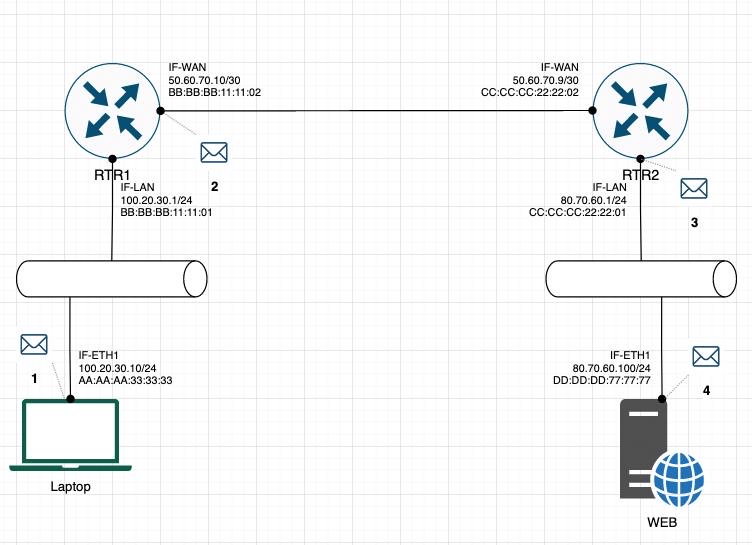
system to 8.8.8.8.



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

* Answer: To see if a connection exists between two devices.
* HTTP – TCP80
* SNMP – UDP161
* HTTPS – TCP443
* DNS client - UDP53?
* DNS zone transfer – TCP53
* SMTP - TCP25
* SSH – TCP22
* FTP – TCP21 (Port 21 is for the control channel, and port 20 is for the data channel)
* Telnet – TCP23
* MSSQL - TCP1433
* MySQL – TCP3306
* PostreSQL - TCP 5432
* RDP (Remote Desktop Protocol) - TCP3389
* NTP - TCP123
* NFS - 2049TCP (depends on the version)

Exercise 2 – TCP/IP Basics



1. The laptop initiates communication with the web server and prepares a packet. What would the packet look like at this stage?

 SRC IP **100.20.30.10/24**

 DST **80.70.60.100/24**

 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 IFWAN.

What would the packet look like at this stage?

 SRC IP **100.20.30.10/24**

 DST IP **80.70.60.100/24**

 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 IFLAN.

What would the packet look like at this stage?

 SRC IP **100.20.30.10/24**

 DST IP **80.70.60.100/24**

 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 **80.70.60.100/24**

 DST IP **100.20.30.10/24**

 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: randomly selected by the browser(or what are we using at the moment) 1024 and above

 DST PORT: 433TCP 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: 433TCP

 DST PORT: randomly selected by the browser(or what are we using at the moment) 1024 and above

How many broadcast domains are there in the exhibit shown? 3

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

network packets

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): Source Address: 192.168.1.101

2. What is the destination IP? (target website): Destination Address: 146.75.0.155

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

screenshot from it:

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

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

from it:

Graphical user interface, text, application

Description automatically generated

Identify the Transport Layer 4 section of the ACK packet and paste a screenshot

from it bellow:

Graphical user interface, text, application

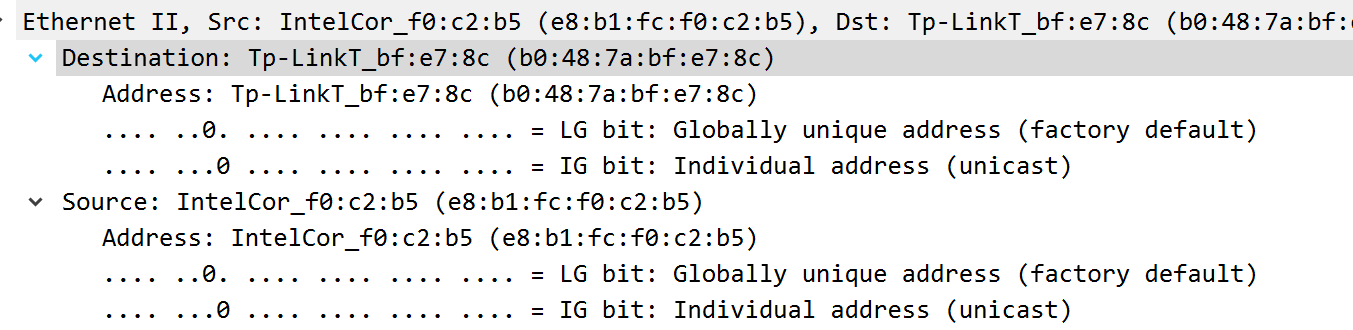
Description automatically generated

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?

My laptop.



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.

Graphical user interface, text, application

Description automatically generated