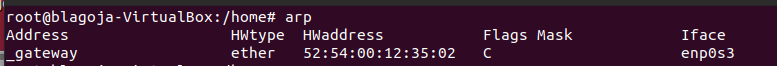
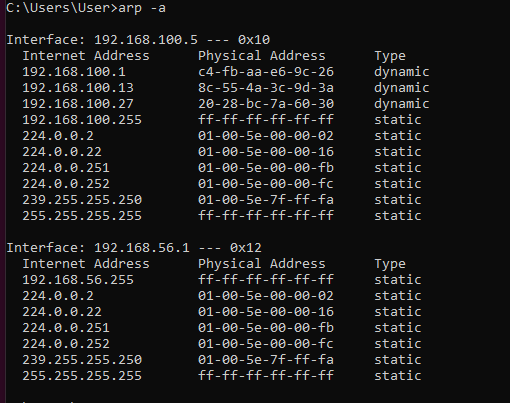
Exercise 1 – Basic network stuffDifficulty: EasyUse the arp command and paste the output from the arp table on your system:

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a media access control (MAC) address.

Linux:



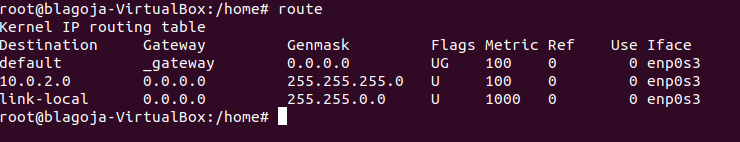
Windows:



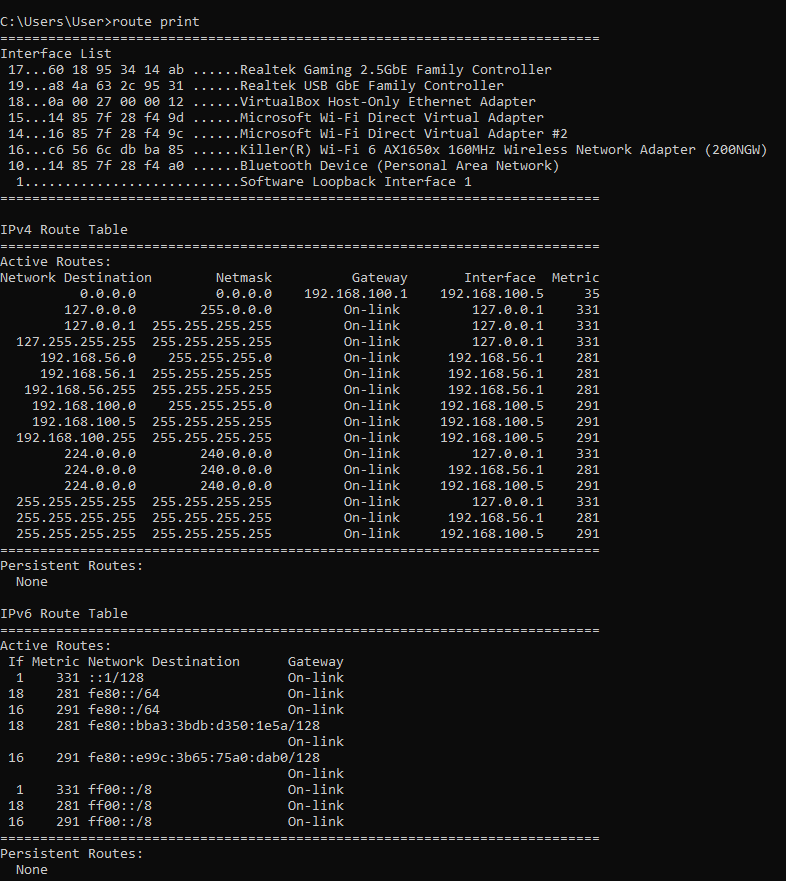
Use the route command and paste the output from the routing table on your system:

It shows and allows to manipulate the IP routing table.

Linux:

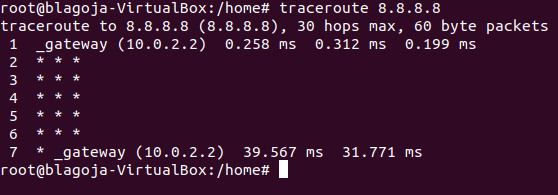


Windows:



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.

Linux:



Windows:



Why would you need to use the ping command?Answer:

The ping command is used to test the connectivity and the reachability of a network device or a host in a network. It sends an ICMP (Internet Control Message Protocol) echo request to the device or the host and waits for an ICMP echo reply.

There are several reasons why you would need to use the ping command:

To test network connectivity: You can use the ping command to verify that you have connectivity to a particular network device or a host. If you can successfully ping the device or the host, it means that there is a working network connection between your computer and the destination.

To troubleshoot network issues: If you are experiencing network issues, you can use the ping command to test the connectivity between your computer and other network devices or hosts. If you are unable to ping a device or a host, it can help you identify where the issue might be occurring.

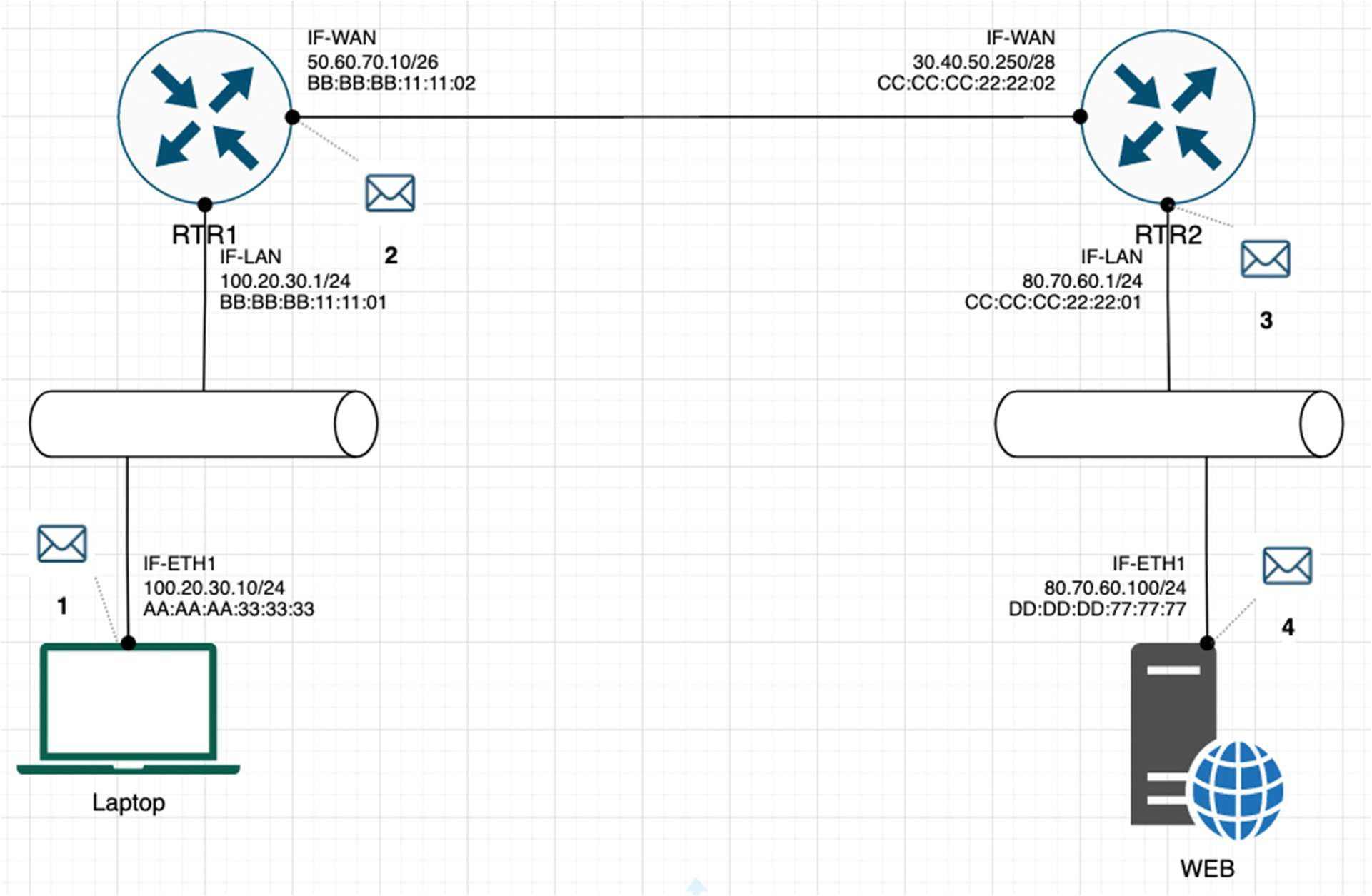
To measure network latency and packet loss: The ping command displays the round-trip time (RTT) for each ICMP echo request and echo reply, which can be used to measure network latency. You can also use the ping command to measure packet loss, which can help you identify issues with network congestion or network performance.

To verify DNS resolution: You can use the ping command to verify that a hostname resolves to the correct IP address. By pinging the hostname, you can confirm that the IP address that is returned by the DNS server is the correct one.

Overall, the ping command is a useful tool for network troubleshooting and performance testing.

Write down the TCP/UDP ports of the most commonly used services bellow in theform of TCP[PORT] or UDP[PORT].As an example, the first two answers have been filled in:  
• HTTP – TCP80  
• SNMP – UDP161  
• HTTPS - TCP443  
• DNS client - UDP53/TCP53 port range 1024-65535  
• DNS zone transfer - UDP53/TCP53  
• SMTP - TCP25  
• SSH - TCP22  
• FTP - TCP21  
• Telnet- TCP23  
• MSSQL – TCP1433 + TCP1434/UDP1434  
• MySQL- TCP3306  
• PostreSQL - TCP5432  
• RDP (Remote Desktop Protocol) - TCP3389  
• NTP - UDP123  
• NFS - TCP2049

**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 IFWAN. What would the packet look like at this stage?

 SRC IP 100.20.30.1

 DST IP 80.70.60.100

 SRC MAC BB:BB:BB:11:11:01

 DST MAC CC:CC:CC:22:22:01

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 100.20.30.1

 DST IP 80.70.60.100

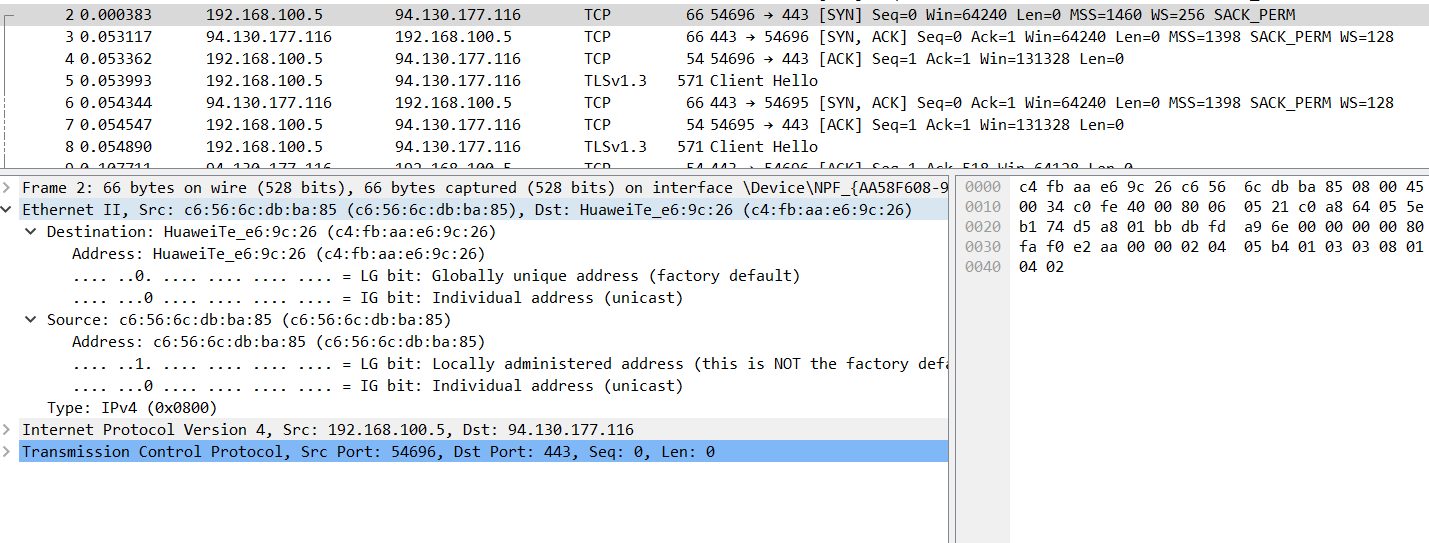
 SRC MAC CC:CC:CC:22:22:01

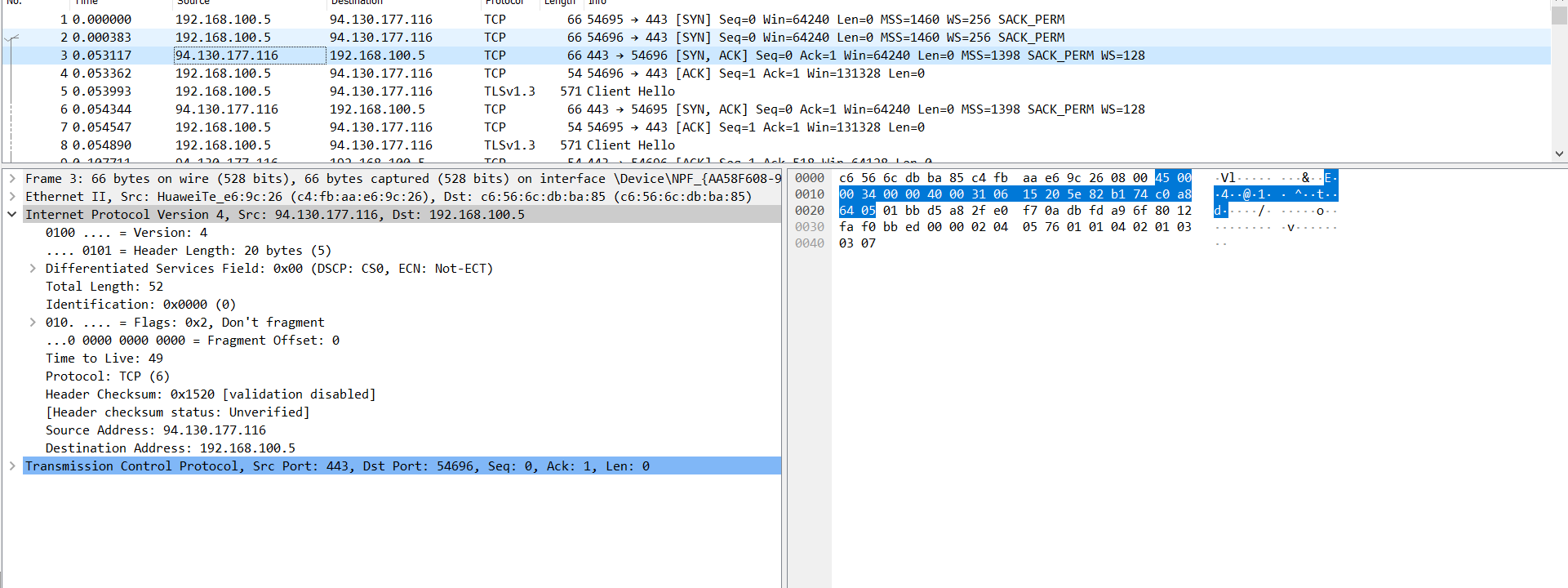
 DST MAC DD:DD:DD:77:77:77

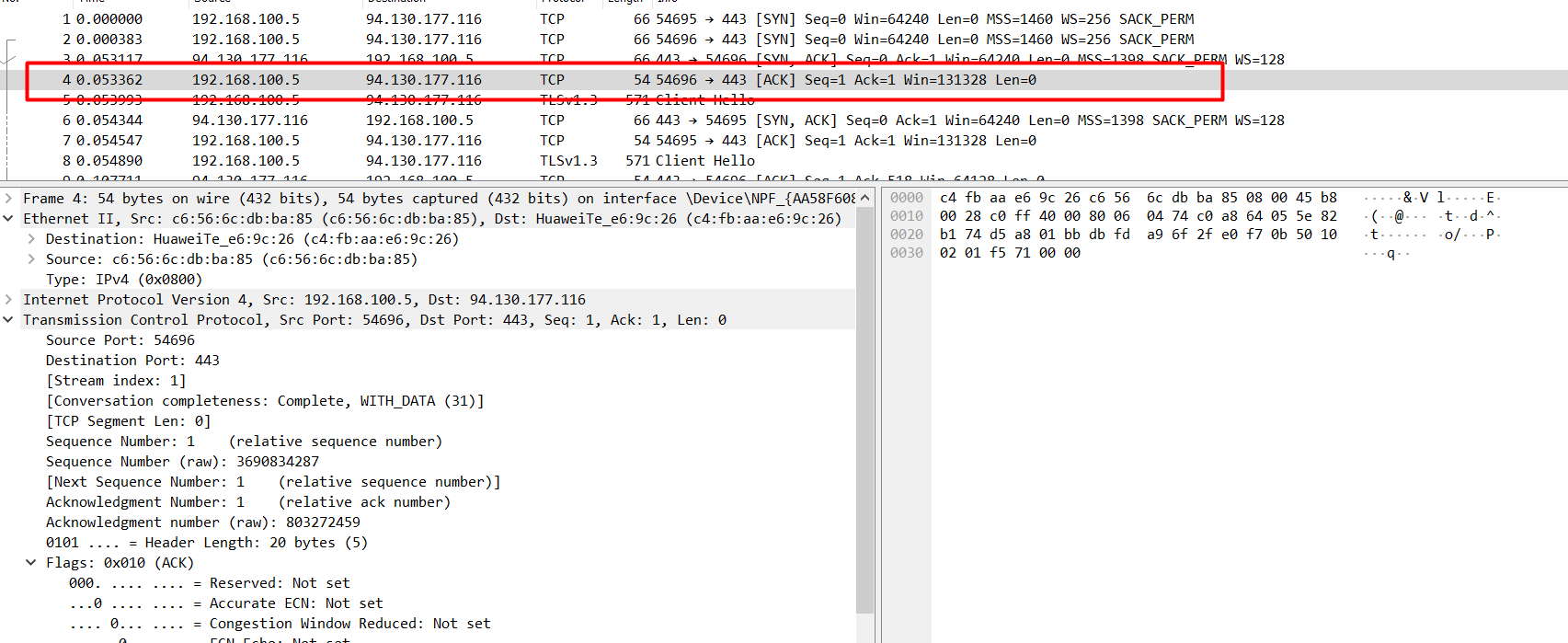
4. The web server receives the packet and prepares a response packet back. What would the packet  
look like at this stage?  
♣ SRC IP 80.70.60.100  
♣ DST IP 100.20.30.10  
♣ SRC MAC DD:DD:DD:77:77:77  
♣ DST MAC CC:CC:CC:22:22:01  
**Since we are talking about web traffic (www) in the example, which transport layer  
protocol will most probably be used?  
θ TCP** - correct  
θ 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: 1024 and above  
• DST PORT: 443 /80 depending if it is HTTPS or HTTP  
**Similarly, and vice versa, what can we expect to see as destination ports when the  
Web server sends a response packet back?**• SRC PORT: 443/80 depending if it is HTTPS or HTTP  
• DST PORT: 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 bellow:**1. What is the source IP (of the initiating host):192.168.100.5  
2. What is the destination IP? (target website) : 94.130.177.116

**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?**

