TLEN 5410 – Network Management and Operations

Lab 3

DHCPv4, DHCPv6 - Auto-configuration, Prefix Delegation & Scapy

University of Colorado Boulder

Interdisciplinary Telecom Program

Professor Levi Perigo, Ph.D.

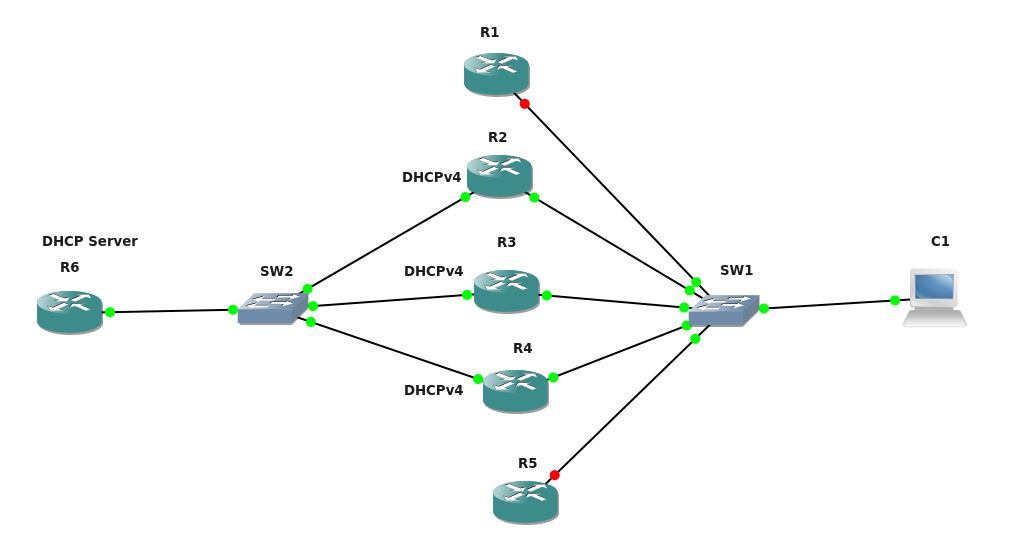
# Summary Introduction to DHCPv4 (Scripting), DHCP Auto-configuration and Prefix-Delegation

This lab focuses on DHCP and provides an insight into IP address configuration in a routed network. We will be using GNS3 to perform all the objectives in this lab. The first part of the lab focuses on configuring DHCPv4 through scripting, and the remaining objectives are intended to instill strong foundation knowledge on DHCPv6. DHCPv6 will be used for auto-configuration of IP addresses and delegating prefixes. In the final part of the lab, different packets are constructed through Scapy.

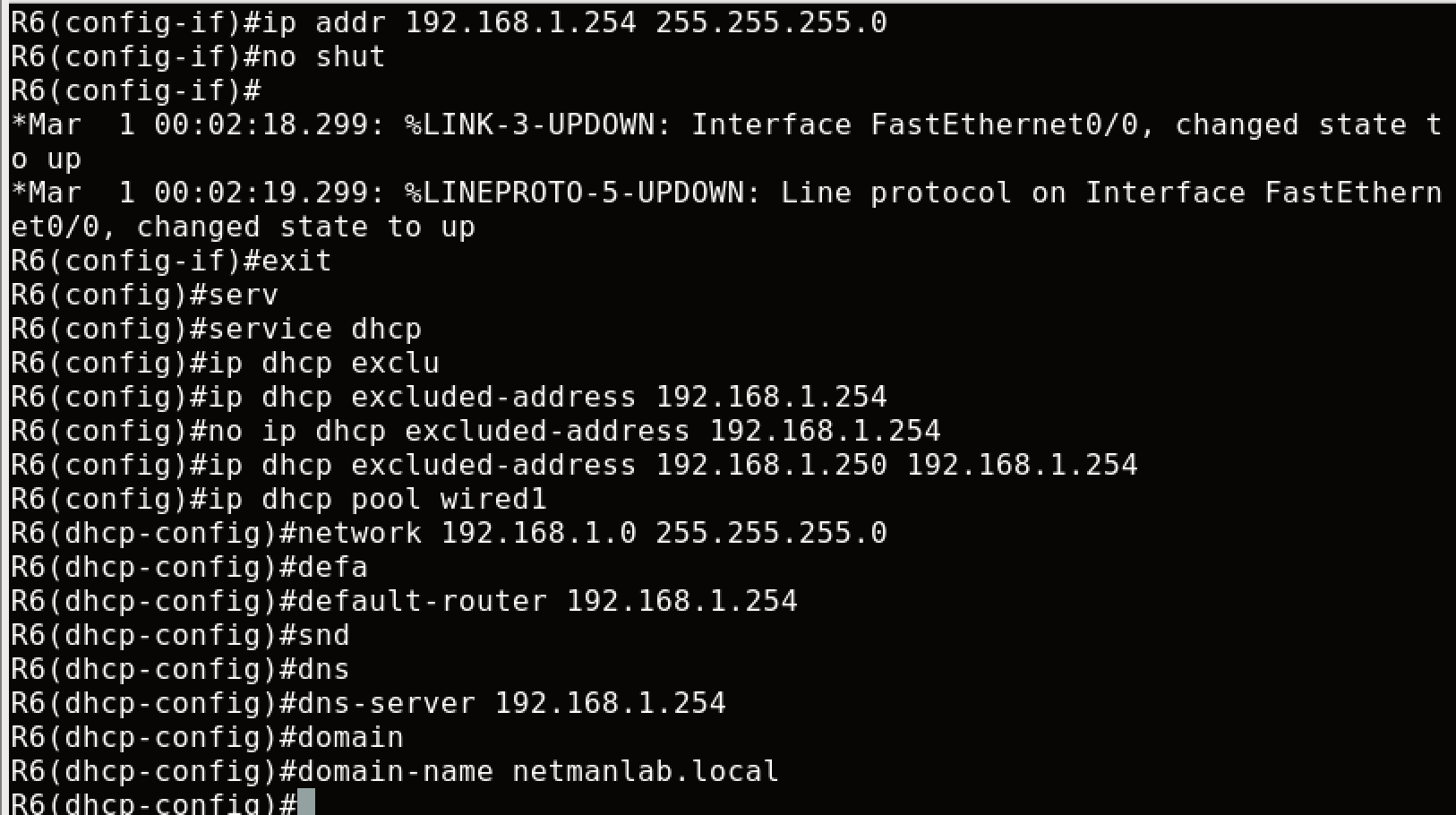
Objectives  
  
PART 1: DHCPv4 Scripting [55 Points]

1. Boot-up the Virtual Machine provided to you for this course. Start GNS3 and create the topology as shown below. (Fig. 1)

Fig. 1

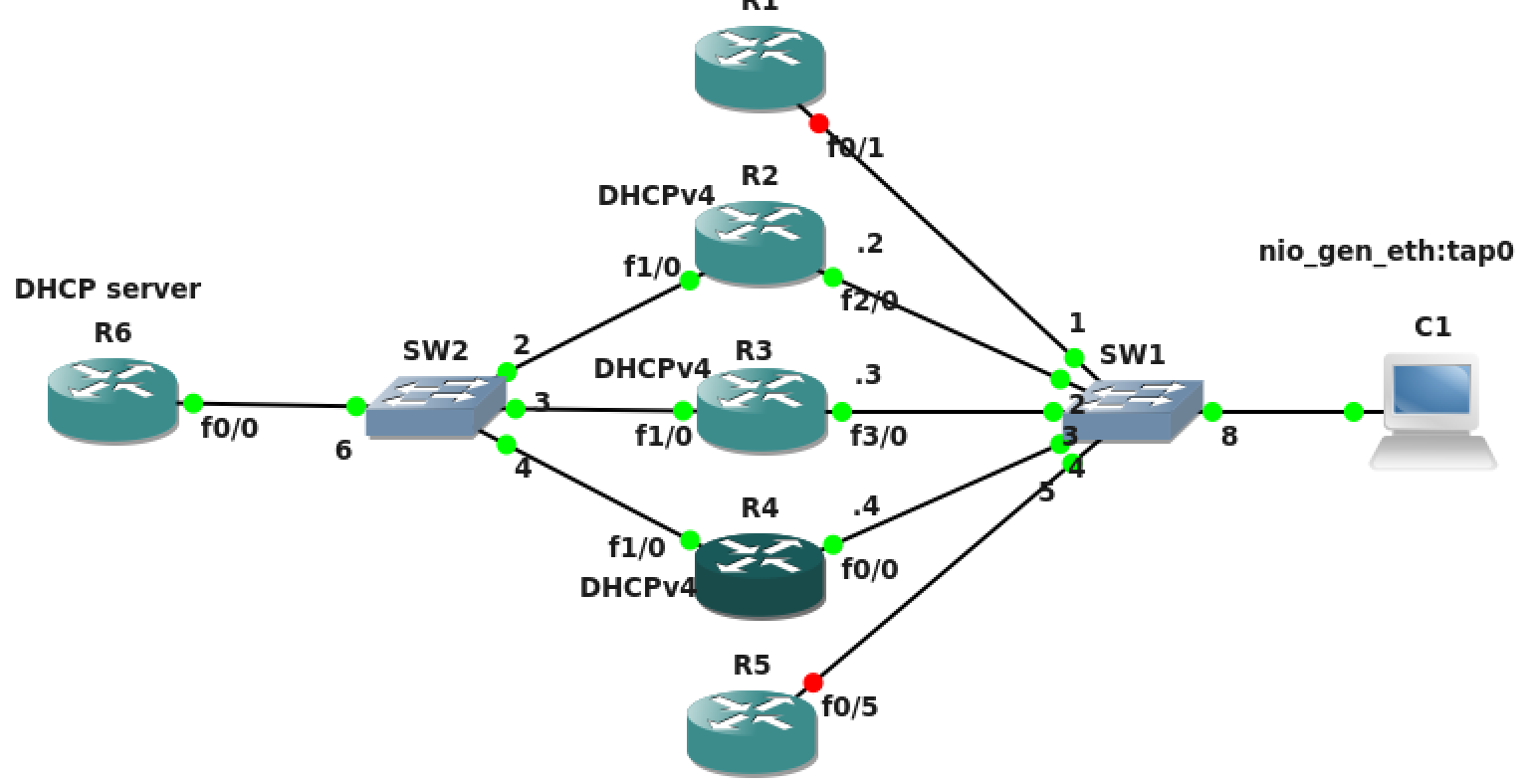


1. Configure R6 to act as a DHCP Server serving IPv4 addresses. Paste relevant screenshot of the configuration. **[5 points]**

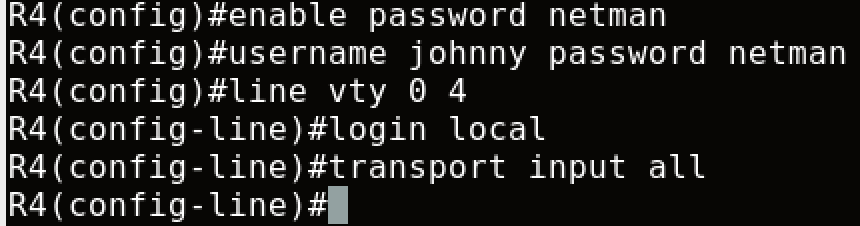
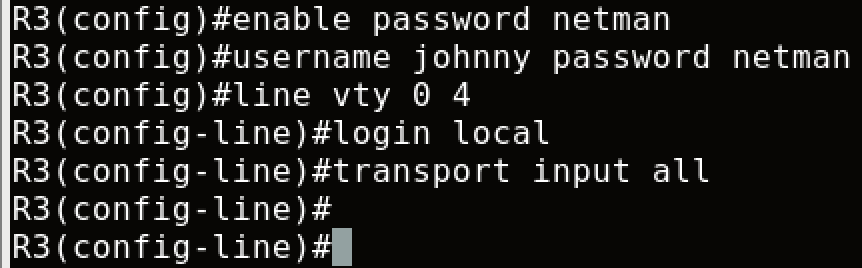
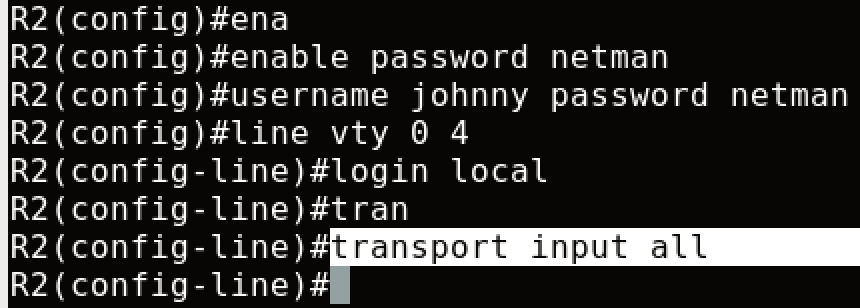


1. Write a Python script **DHCPv4Config.py** to configure DHCPv4 for the interfaces of R2, R3, R4 (facing SW2) to obtain IPv4 addresses from the DHCPv4 server (R6). Your code should facilitate simultaneous login to all three routers and deploy the configuration concurrently. Paste relevant screenshots of the output and submit the script along with the report. **[20 points]**

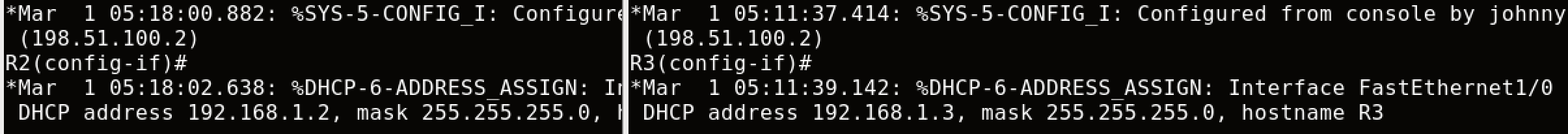
Note: - Please make sure that the DHCP pool subnet you define is different from your existing VM subnet. (198.51.100.0/24)

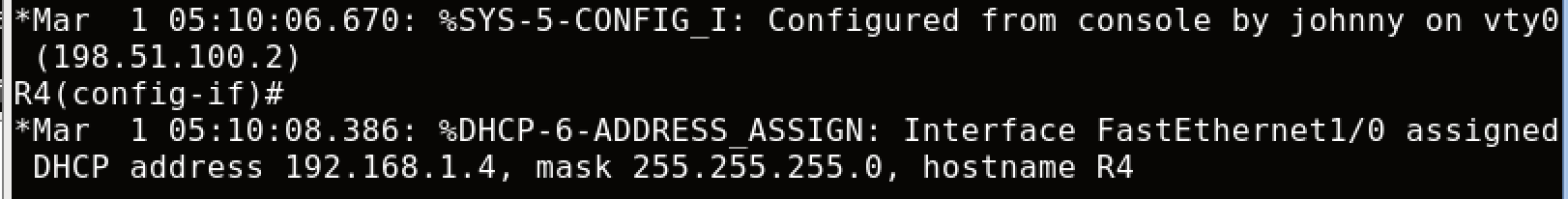


* First I configured the following commands on R2, R3, R4 for ssh connection:
* conf t
* enable password netman
* username johnny password netman
* username johnny priv 15
* line vty 0 4
* login local
* transport input all
* ip domain-name netman.com
* crypto key generate rsa
* 1024
* end
* And then assign IP addresses on the interfaces facing the host like the picture, so that I can ssh into R2, R3, R4

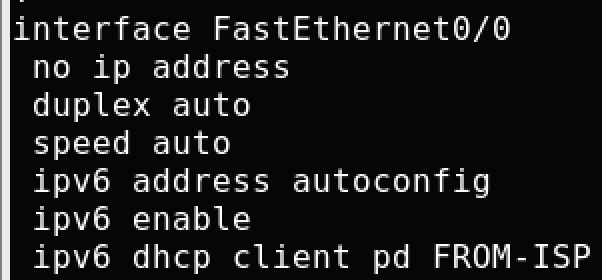


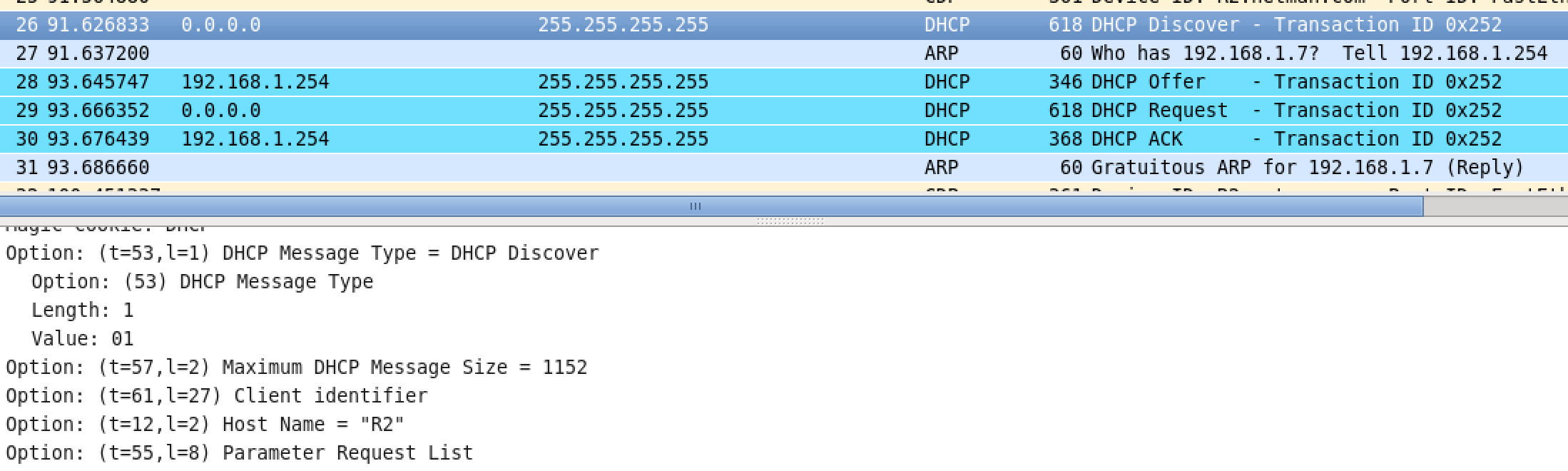
Outputs:

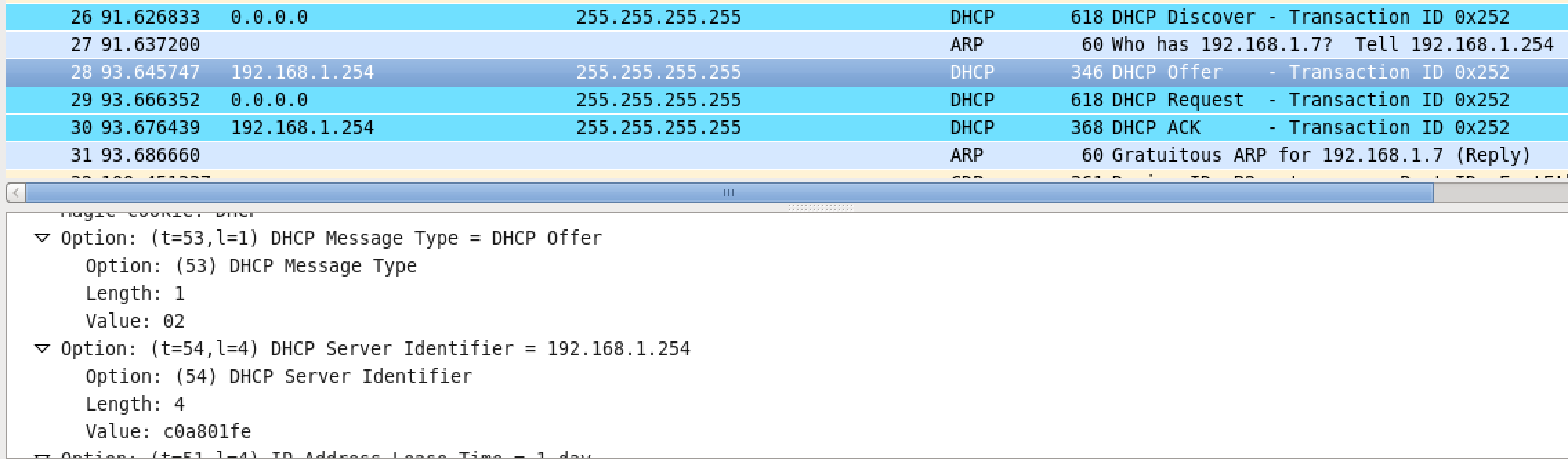


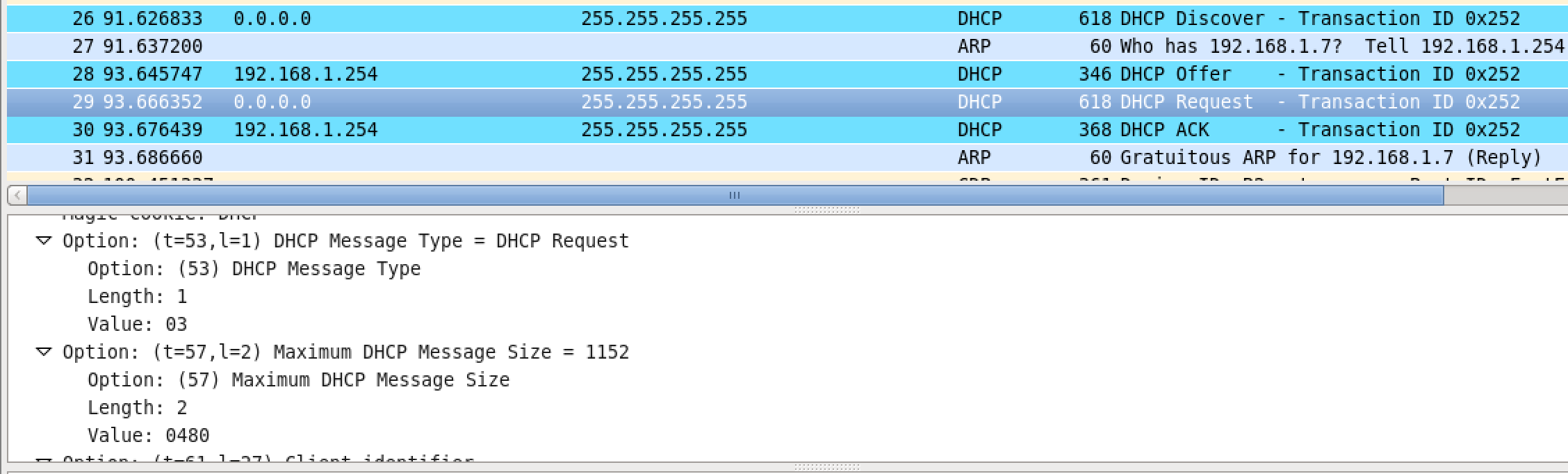


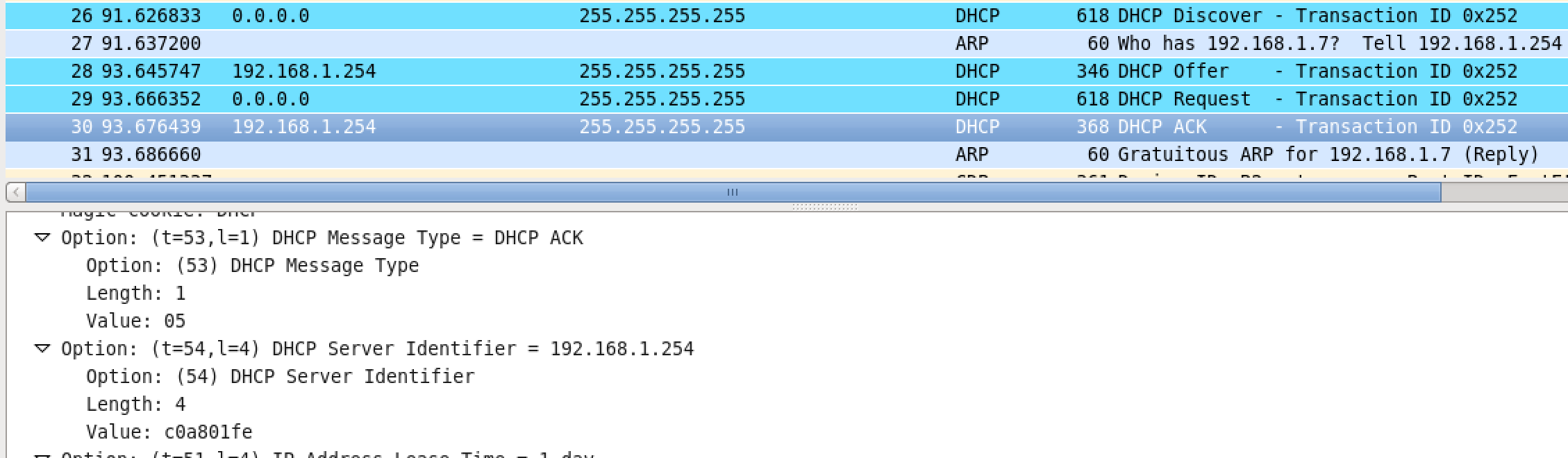
1. Monitor the interface connecting Switch SW2 and the DHCPv4 server (R6) and capture the DHCPv4 DORA messages using Wireshark:
   1. Use appropriate display filter to show the relevant DHCP messages between R2 and R6. Provide screenshots of the expanded packet view of the DORA messages. **[10 points]**



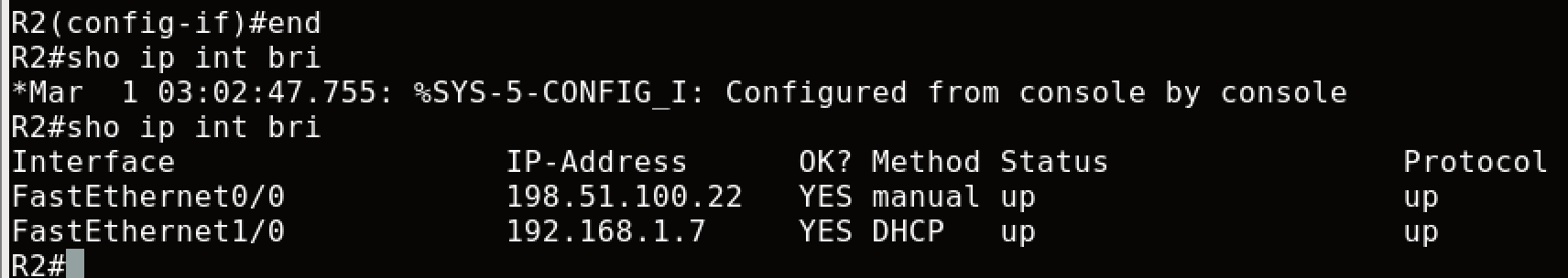


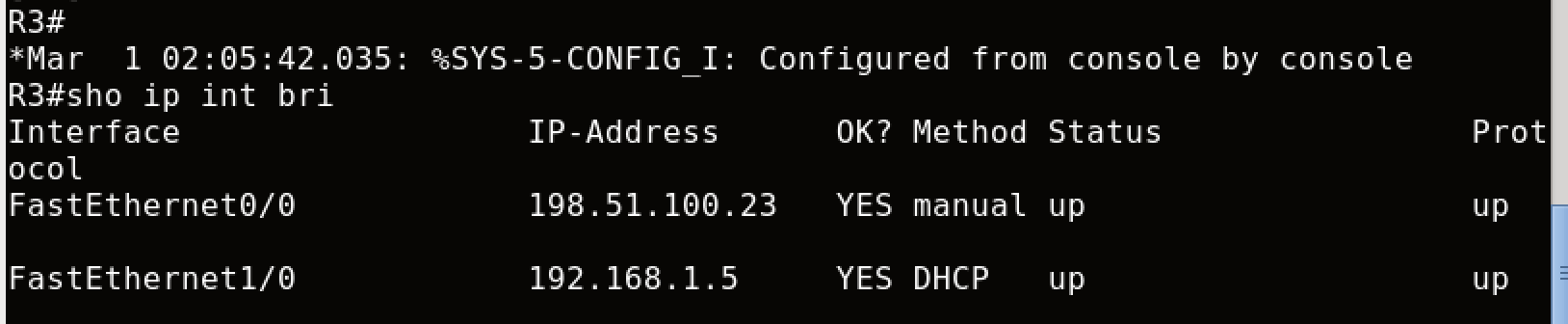


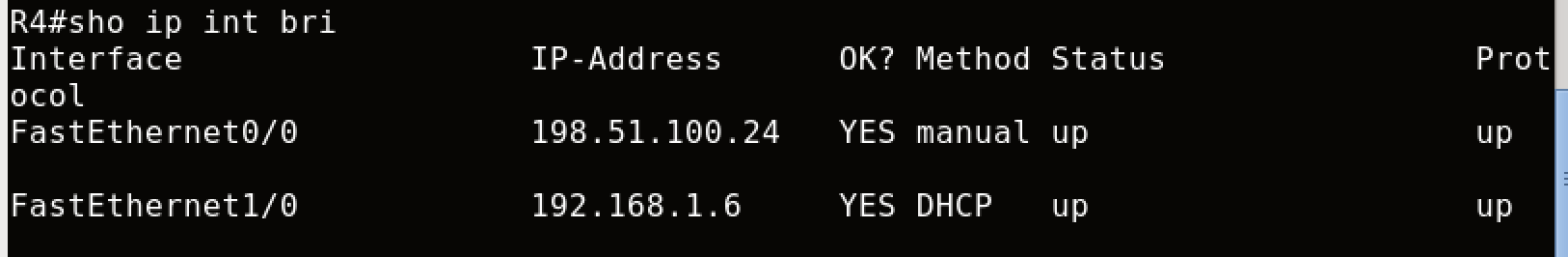


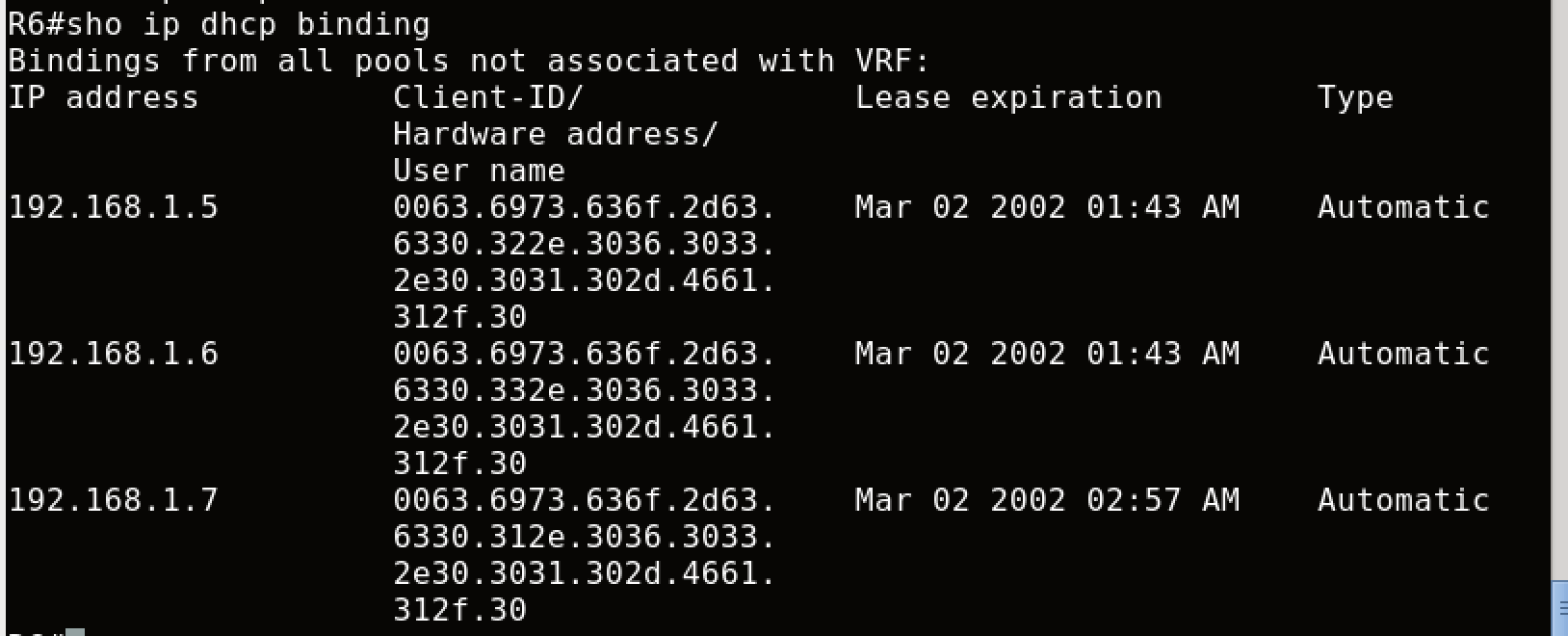


1. Provide a screenshot of the ‘show ip interface brief’ command on R2, R3, and R4 and ‘show ip dhcp binding’ on R6. **[10 points]**





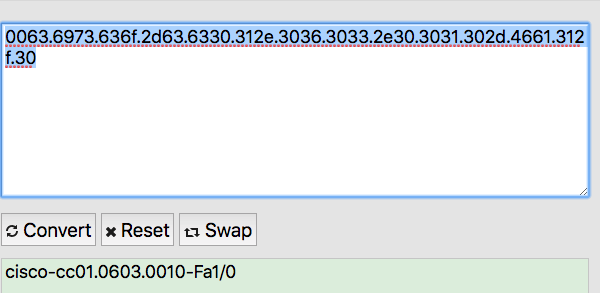


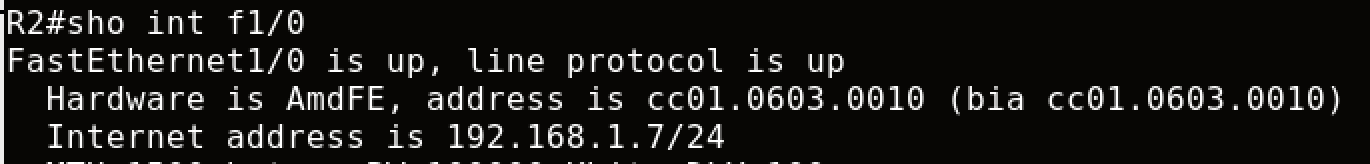


* 1. Does the hardware address match the interface of R2, R3, and R4? Show how you can verify this. **[10 points]**

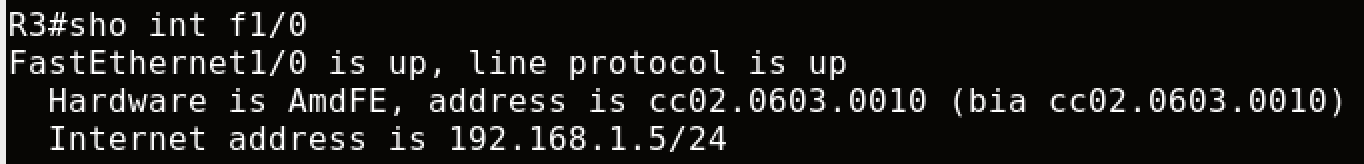
Yes, they match. When I put 192.168.1.7 of hardware address(0063.6973.636f.2d63.6330.312e.3036.3033.2e30.3031.302d.4661.312f.30) into hex to ASCII text translator, you can see the output.

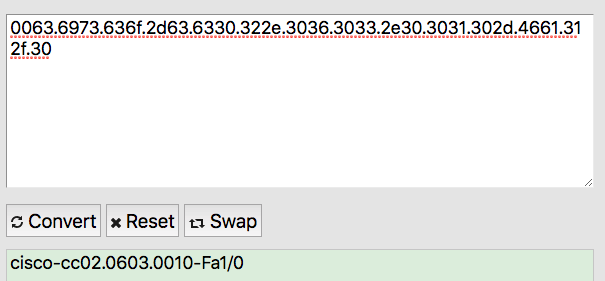
R2:



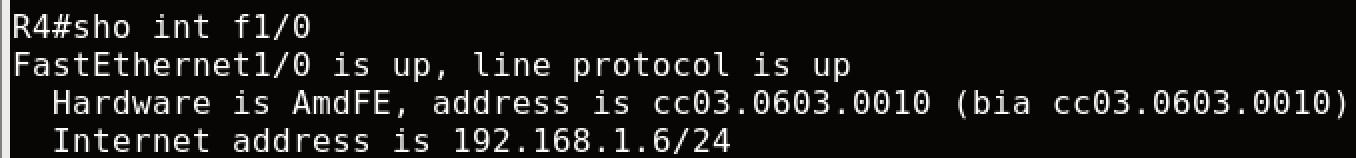


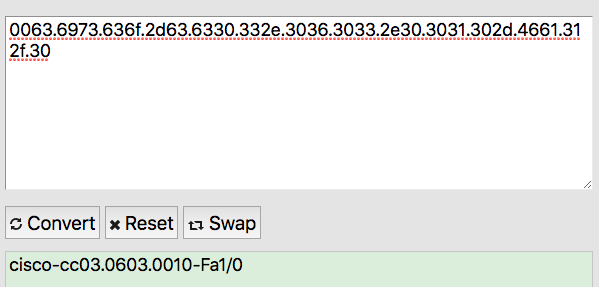
R3:





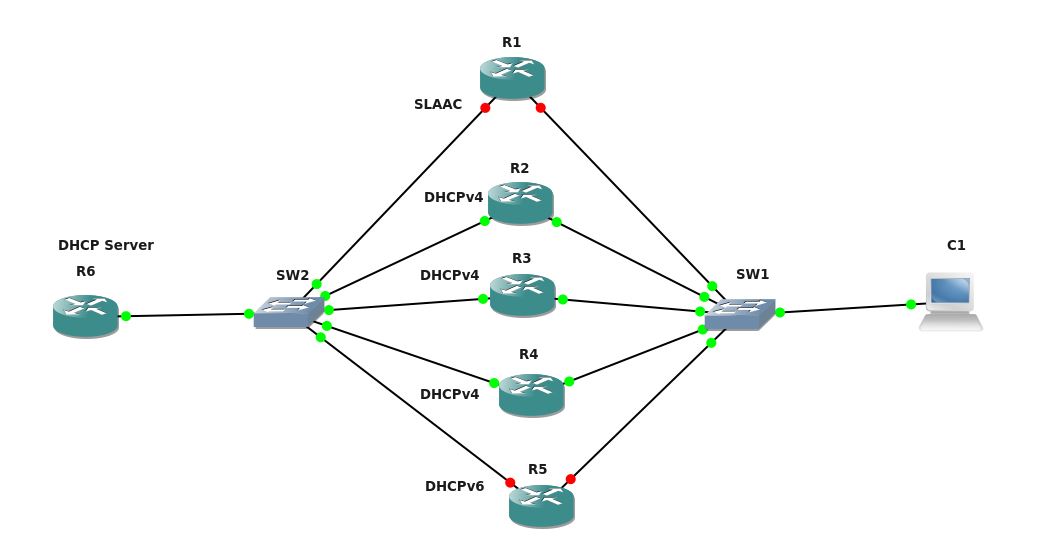
R4:

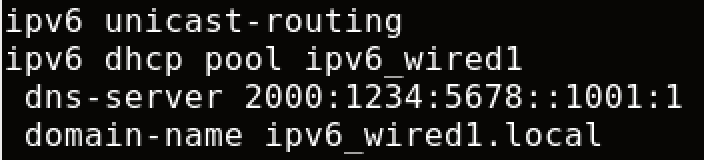


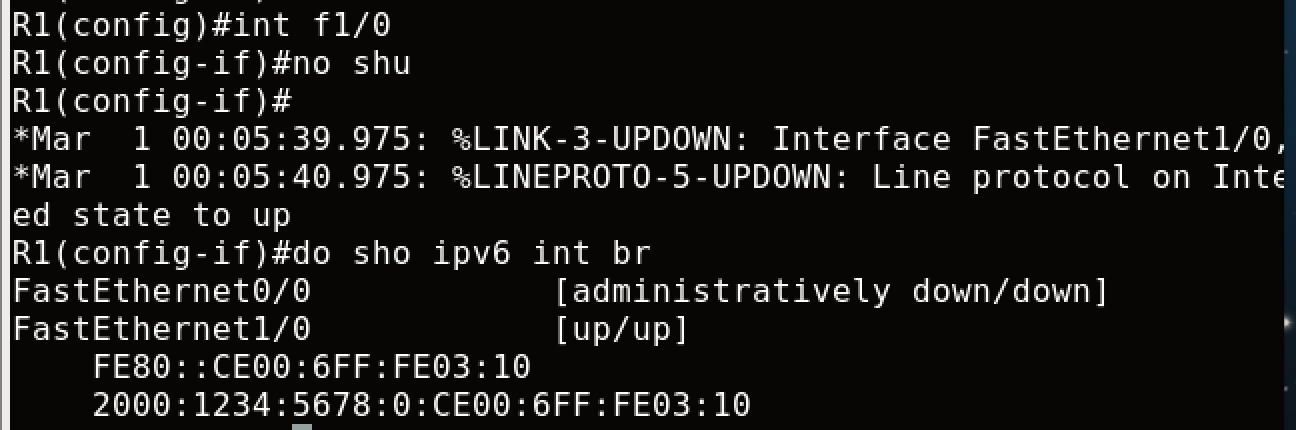


PART 2: DHCPv6 Auto Configuration [30 Points]  
  
IPv6 Auto-configuration Using SLAAC.

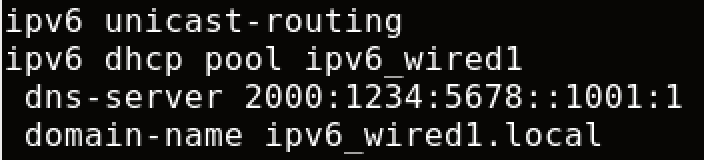
1. Configure the interface of R1 connected to the switch (SW2) to obtain an IPv6 address using SLAAC. **[10 points]**

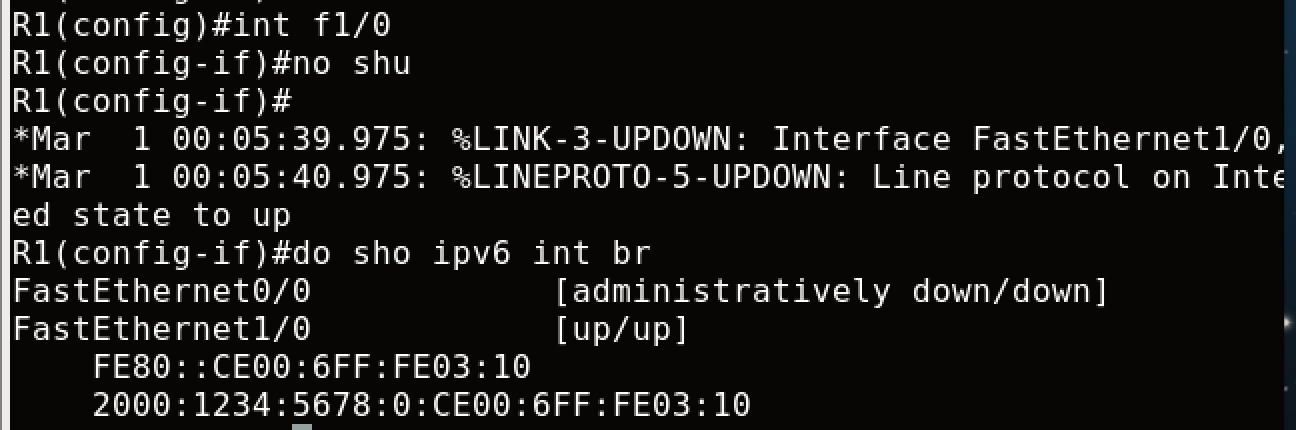


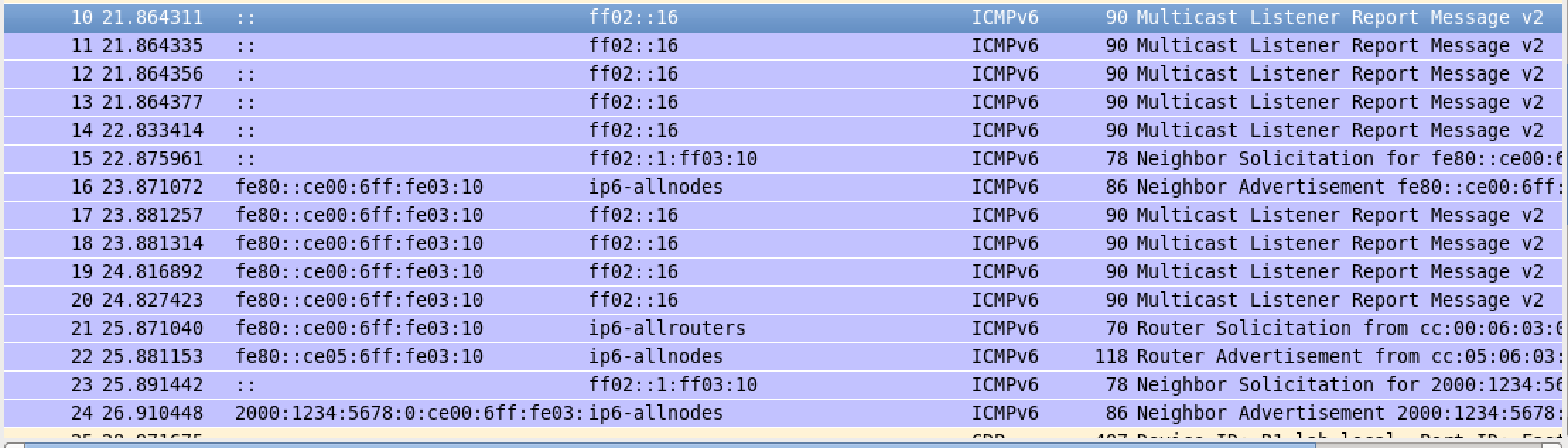




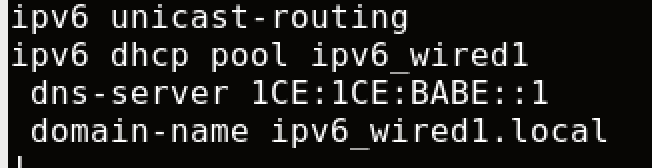
1. Provide a screenshot of the IPv6 configuration commands (on R6 and R1, as well as the Wireshark capture that shows R1 obtaining an IPv6 auto-configuration address. **[10 points]**

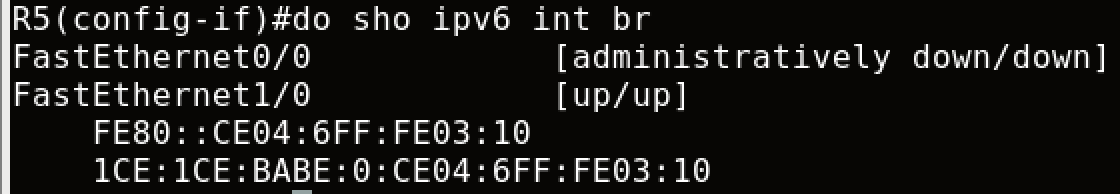


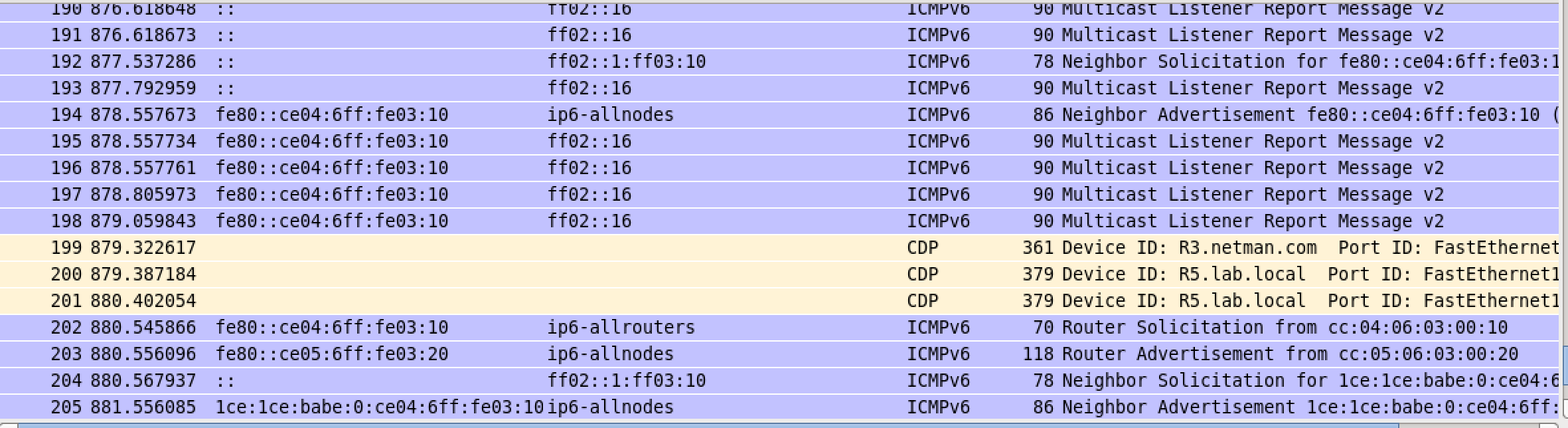




1. Configure R5 for DHCPv6 stateless. R5 should receive the DNS server IP address of 1ce:1ce:babe::1 from the DHCPv6 server (R6).
2. Provide a screenshot of the DHCPv6 stateless configuration on R6, and the Wireshark output from R5 indicating it received the DNS address via DHCPv6. [**10 points**]







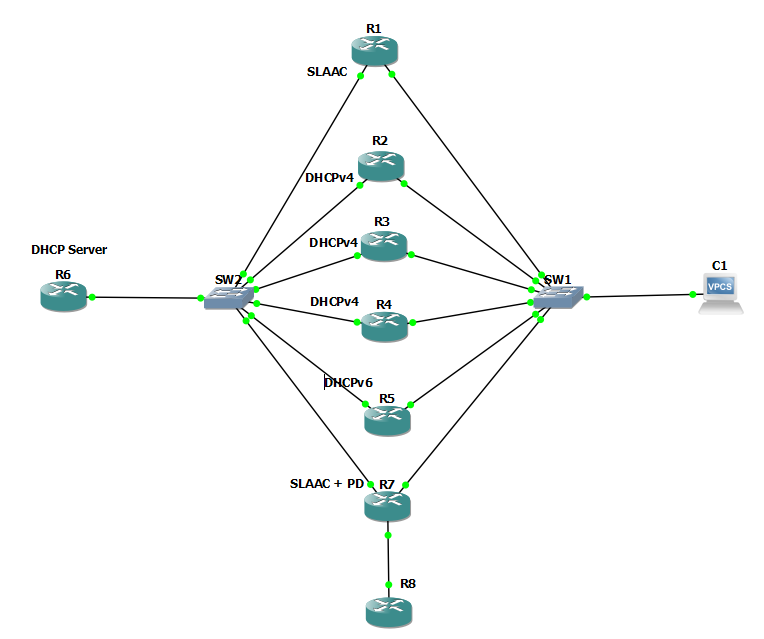
# PART 3 (Optional Objective - Not graded): DHCP Relay

IPv4 DHCP Relay

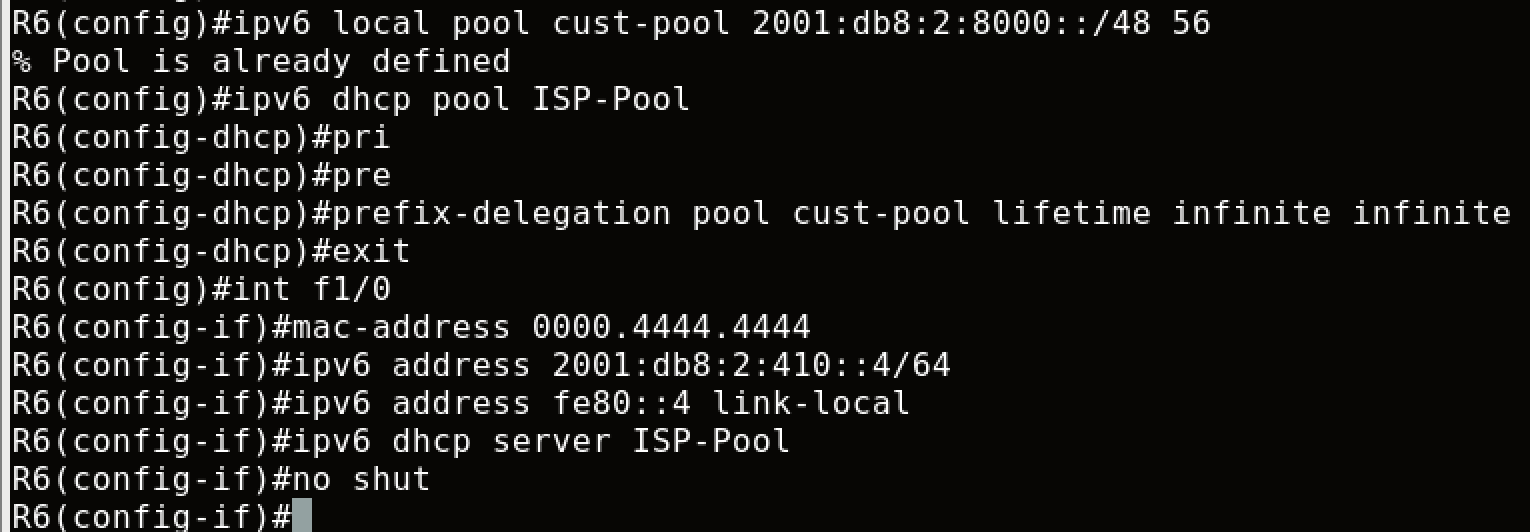
1. Create a network design, where an additional router is added to the network (behind R1). Have this newly added router receive an IP address from the DHCP server, via the DHCP relay.
2. Provide a screenshot of the Wireshark capture showing the client receiving an address via DHCP relay.
3. Provide the relevant router configurations that are required for DHCP relay.

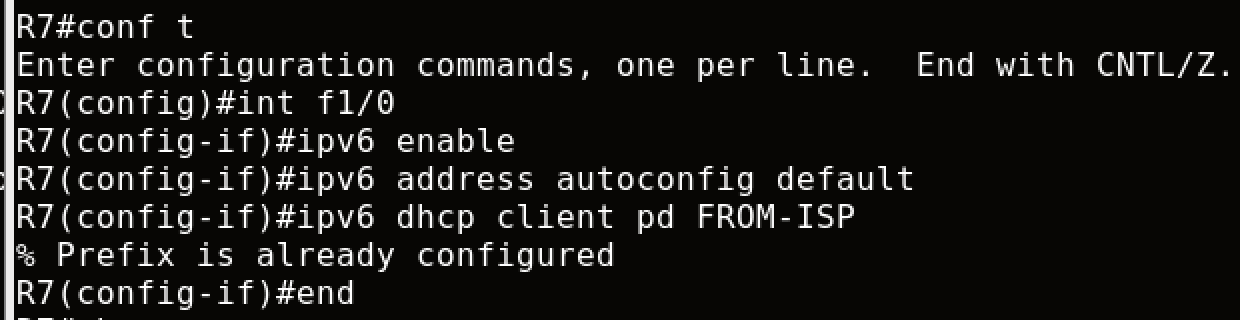
# PART 4: DHCPv6 Prefix Delegation [45 Points]

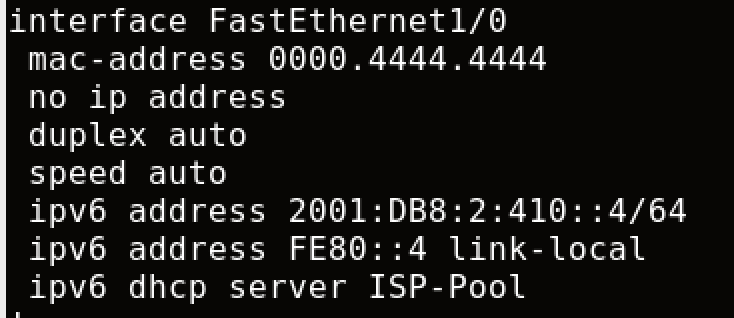
The aim of this objective is to make R6 allocate a prefix to R7 through DHCPv6 Prefix delegation and subsequently make R7 allocate an IPv6 address to R8 from the delegated prefix pool.

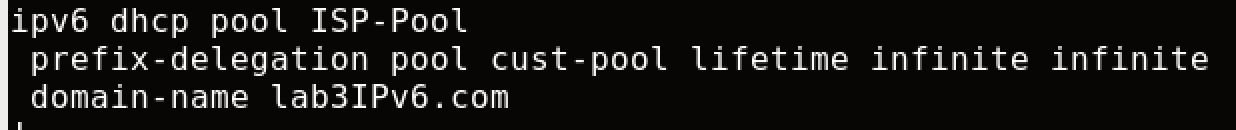


1. Create the topology as shown in the above figure.
2. Configure R6 to act as a DHCPv6 Server to allocate a /48 Prefix to R7. In addition, the interface on R7 connecting to SW2 should receive an IPv6 address through SLAAC. Paste the screenshots of the relevant configuration on both R6 and R7. **[10 points]**



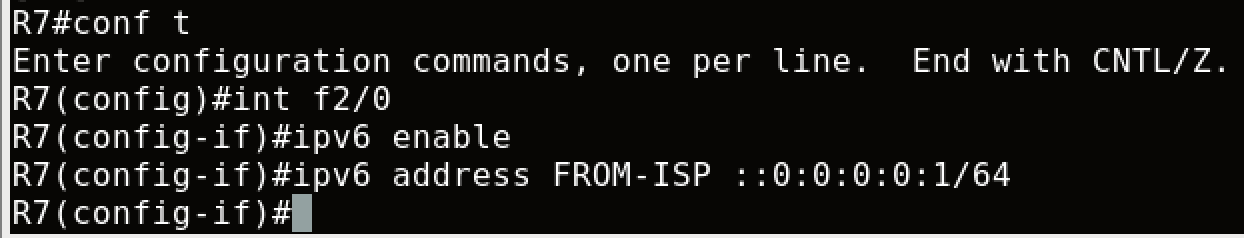


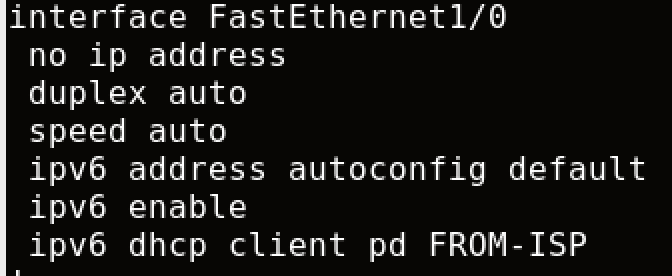




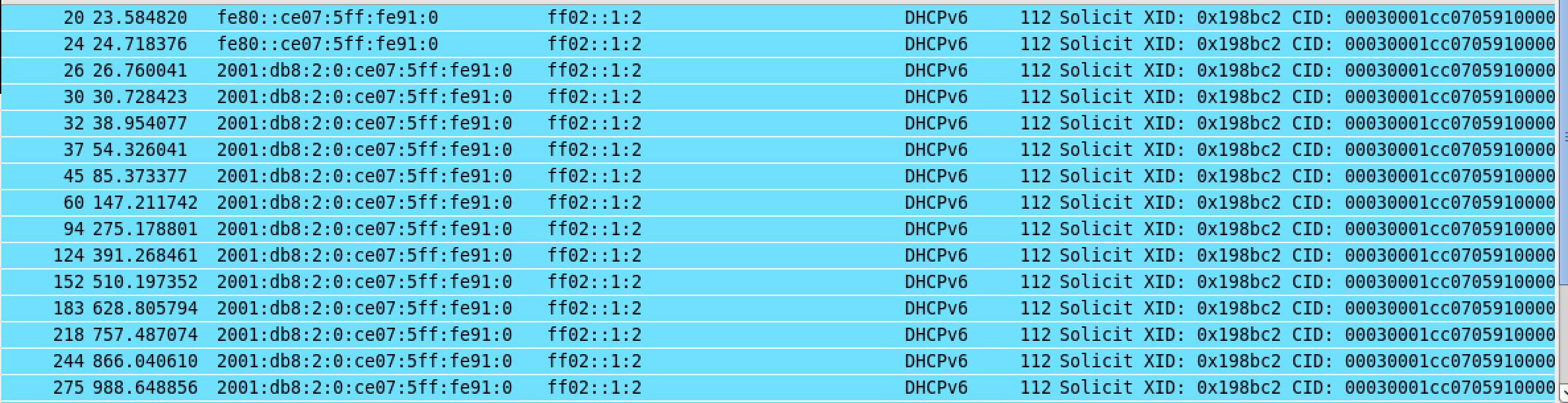


1. Configure R7 and R8 such that R8 receives a /64 address from the prefix pool delegated to R7 in the previous step. Paste the screenshots of the configuration on both R7 and R8. **[10 points]**



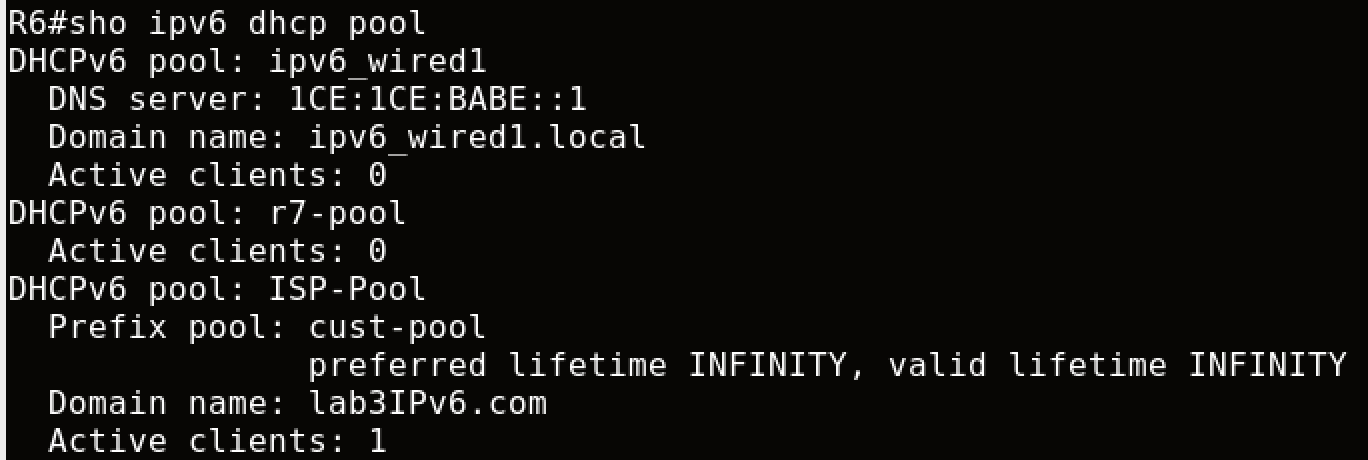


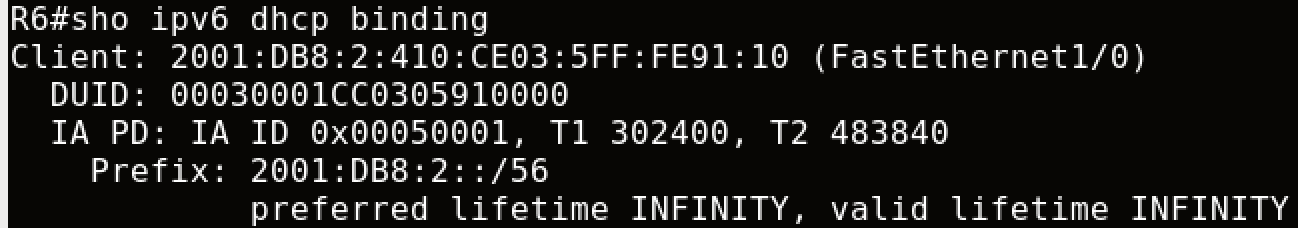
1. Provide screenshots of the Wireshark packet captures showing the prefix delegated to R7 and the address allocated to R8. **[10 points]**



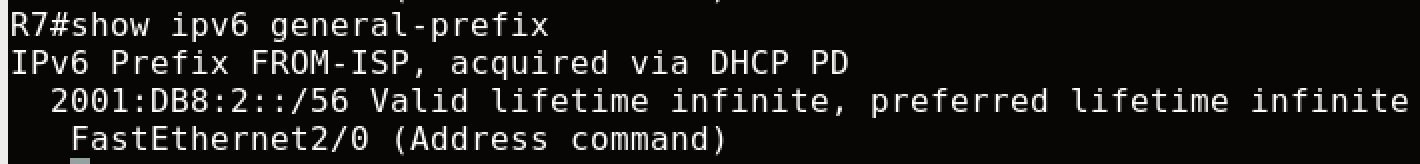


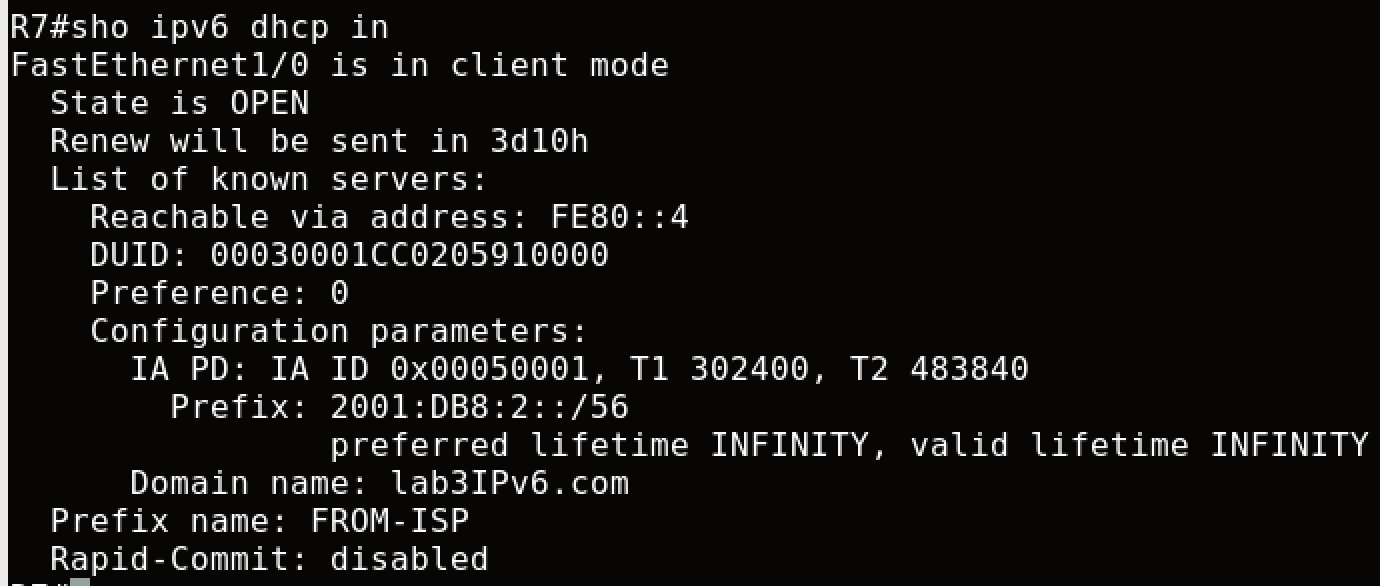
1. Provide a screenshot of the output for the following commands **[15 points]**:
2. “show ipv6 dhcp pool” and “show ipv6 dhcp binding” on R6



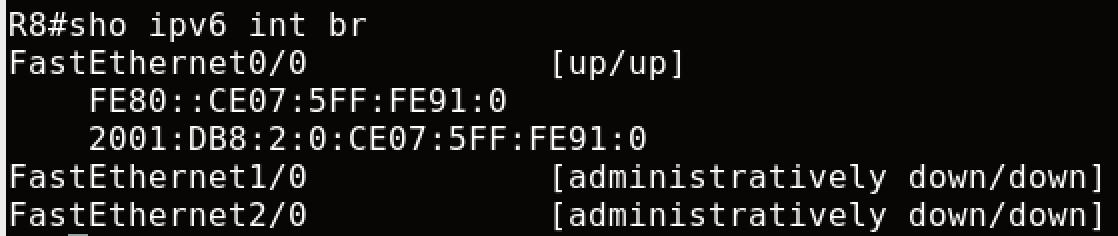


1. “show ipv6 general-prefix” and “show ipv6 dhcp interface” on R7





1. “show ipv6 interface brief” and “show ipv6 interface” on R8

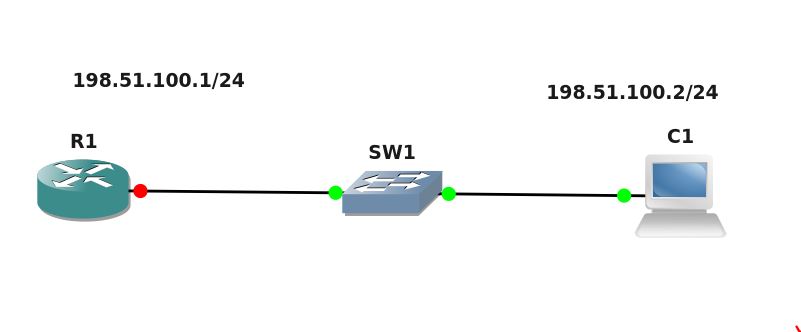




# SCAPY [110 Points]

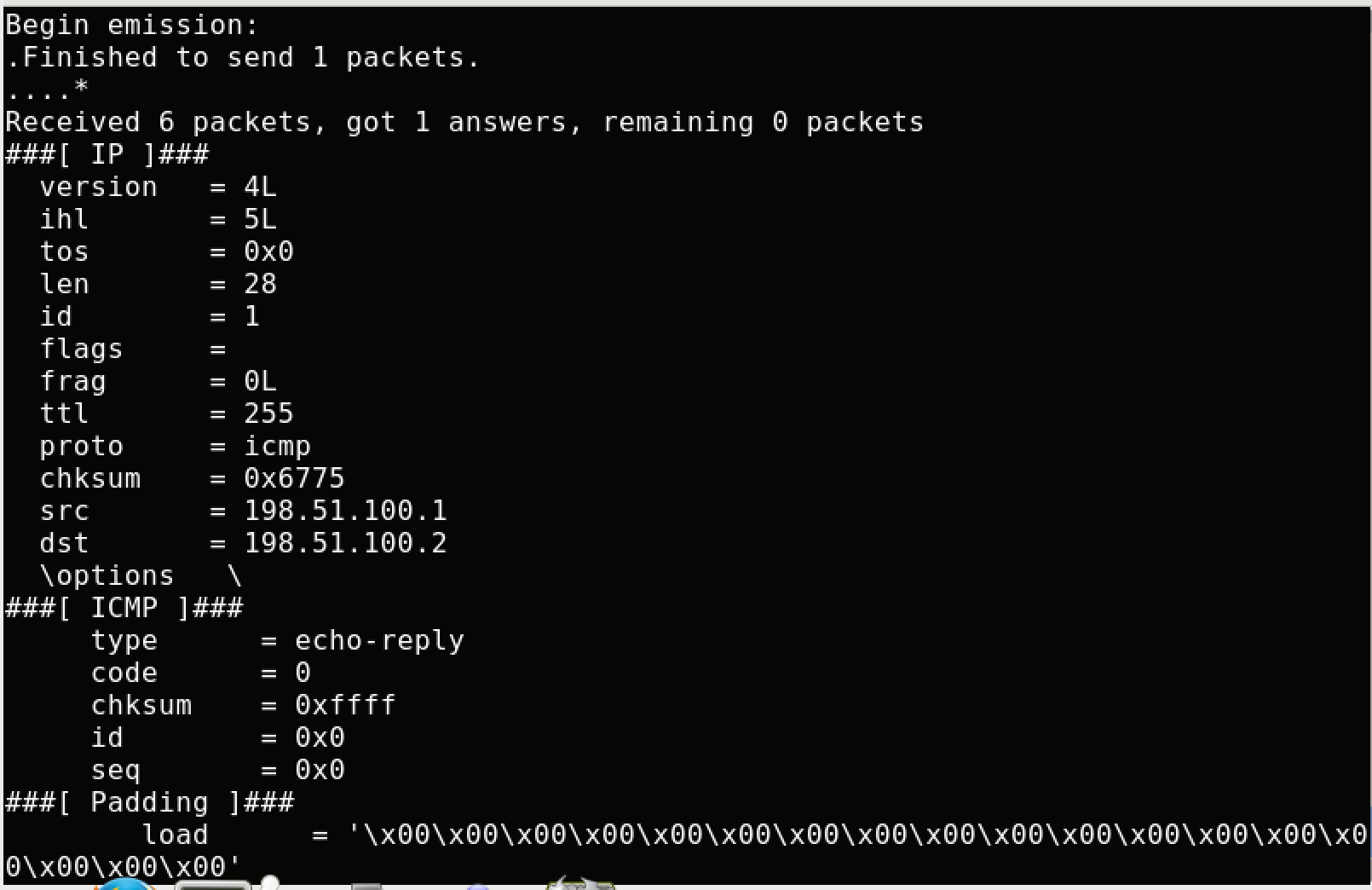
Hackers are constantly adapting to network security techniques. Our network security ingenuity needs to improve and adapt to be able to protect dynamic security attacks. Scapy is one of the tools that gives us the ability to create, forge, and decode our own packets, send them on the network, capture them, and much more. Imagine how useful this tool can be to emulate and study the attacks, analyze the network behavior, and help in developing techniques to keep our networks safe and secure.

Pre-requisites: - Before proceeding with the Scapy lab, create the topology shown below.

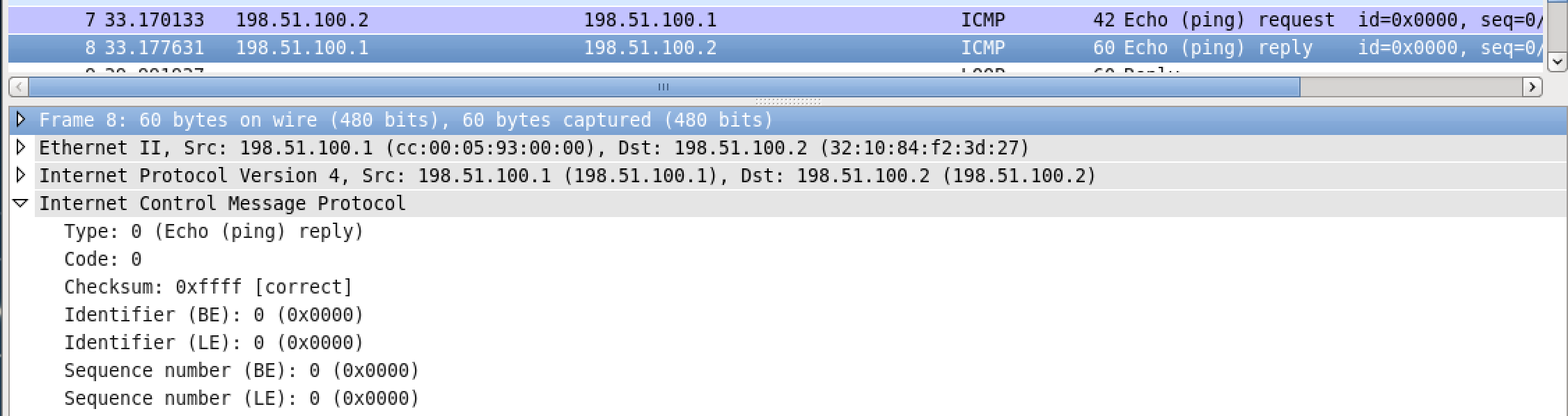


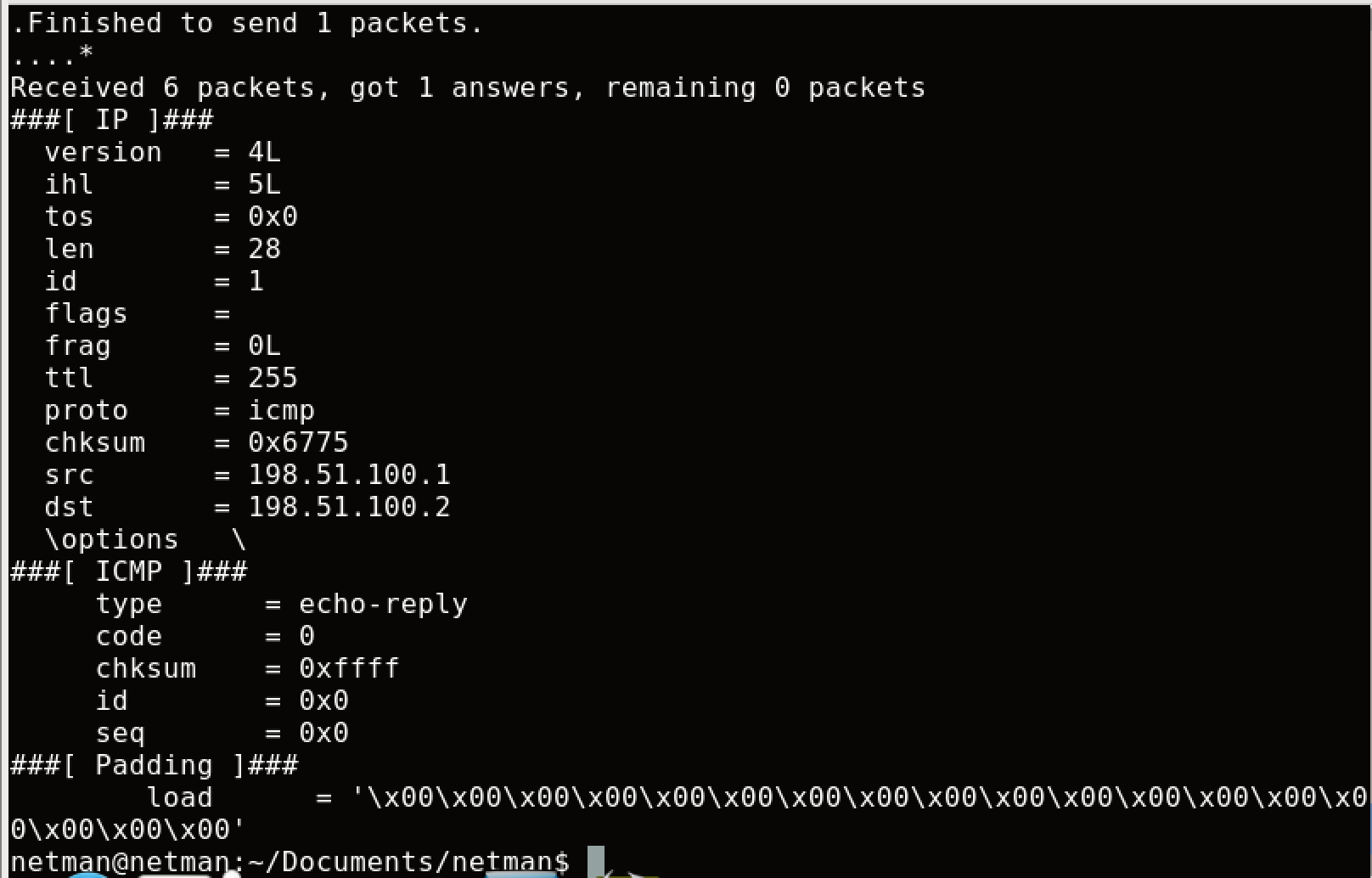
Objective 1: Creating an ICMP echo request packet and ARP frame through Scapy:

1. Create your own ICMP echo request packet on the VM (C1) to ping R1’s interface using Scapy. Show the packet structure in Scapy using appropriate show commands. **[10 points]**

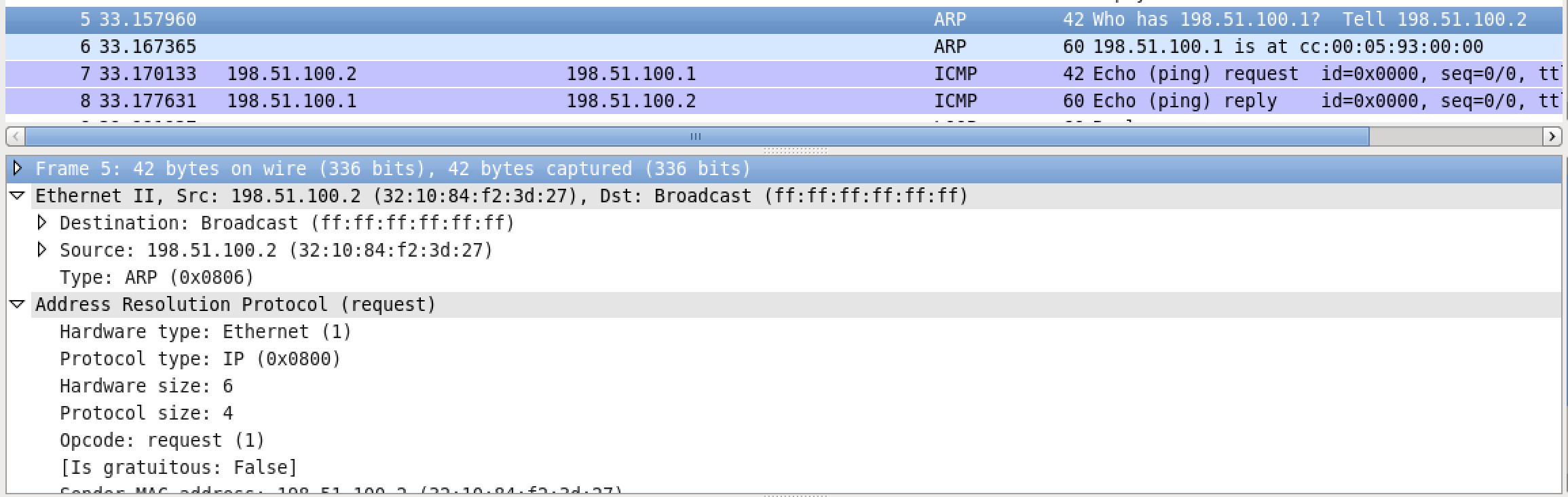


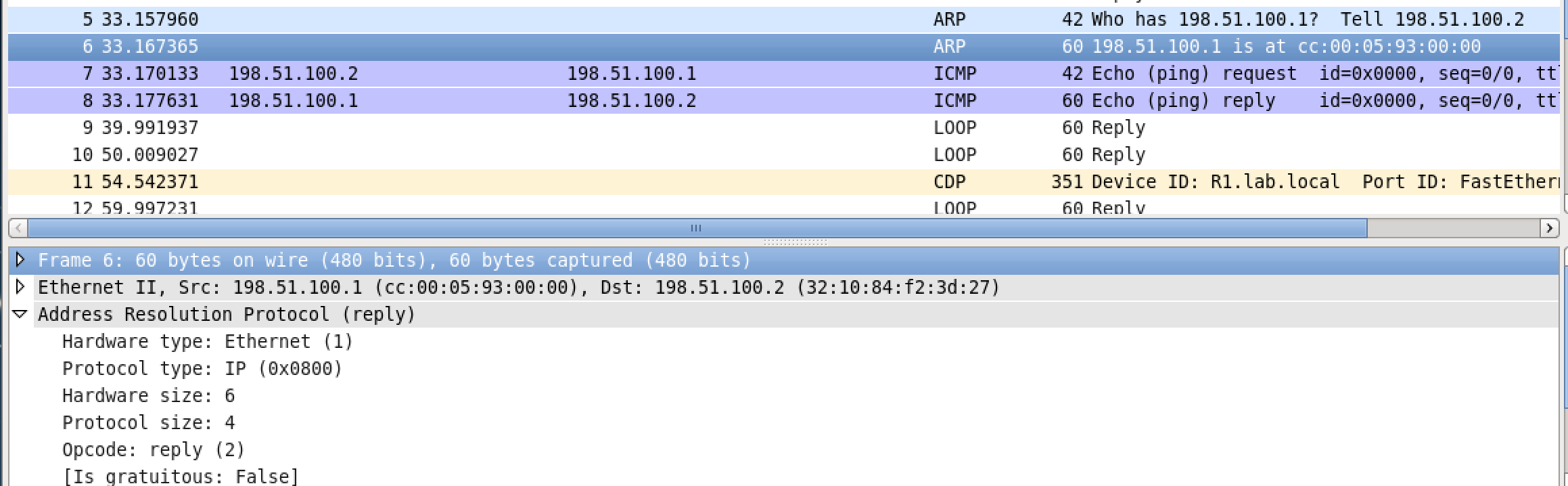
1. Before starting this objective, start a Wireshark capture on the correct interface in the above topology. Now send your Scapy generated echo request packet to router R1. Did you get a response for the above echo request? If yes, show the Wireshark capture indicating the response as well as the packet **received** in Scapy. If no, check if your echo request packet has the correct fields and it is being successfully delivered to R1. Try again after troubleshooting and resolving your issue to complete the objective. **[15 points]**



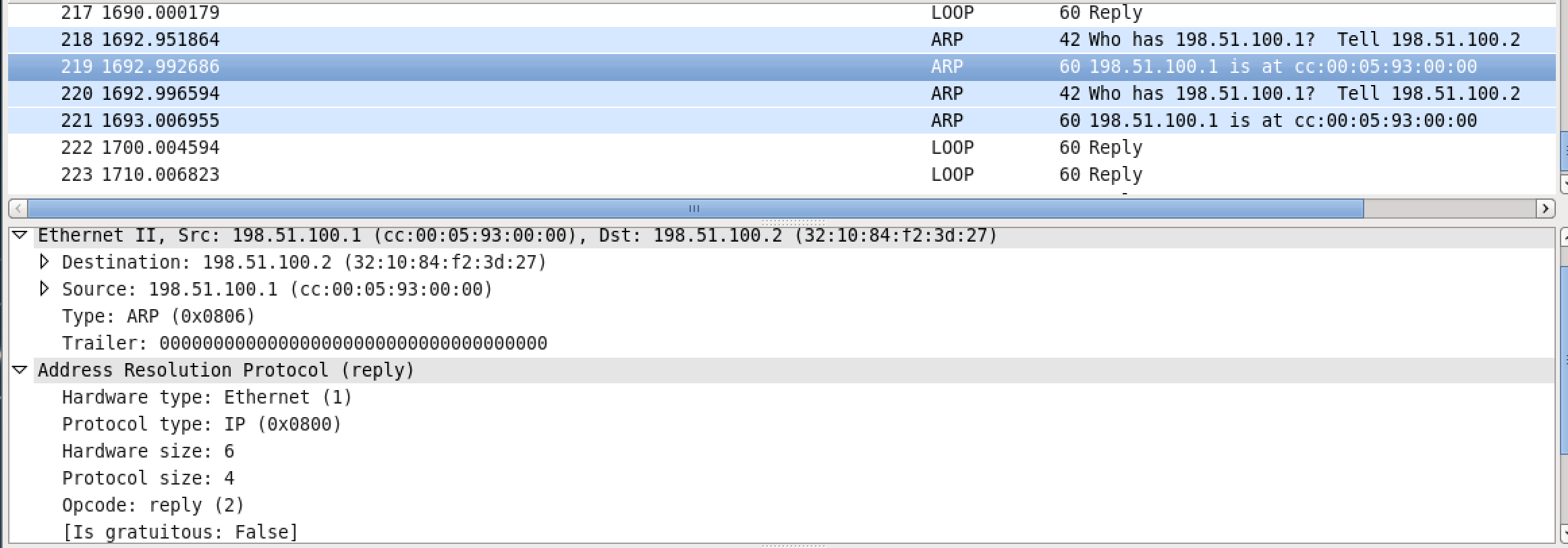


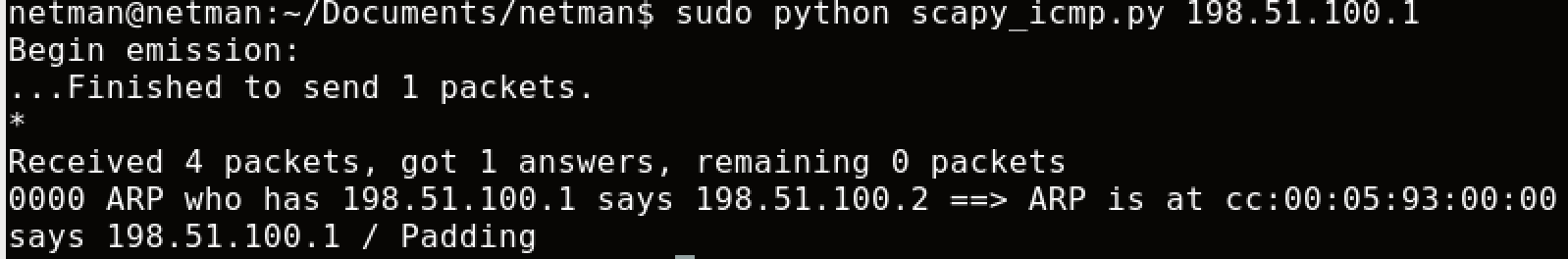
1. Using the Wireshark capture from step 2, filter the ARP exchange messages. Paste relevant screenshots. If you do not see ARP messages from the previous objective in Wireshark, create a new topology as above in GNS3, start Wireshark capture and then initiate a ping to R1 from C1’s terminal. Filter the ARP exchange and show appropriate screenshots. Good understanding of ARP exchange messages and frame format will help you in the next objective. **[10 points]**





1. Start your Wireshark capture in the above topology before starting this objective. Recreate an ARP request destined to router R1 in Scapy and capture the ARP response in Wireshark to find the MAC address of the router. Paste relevant screenshots indicating successful ARP response for your Scapy generated ARP request. **[10 points]**

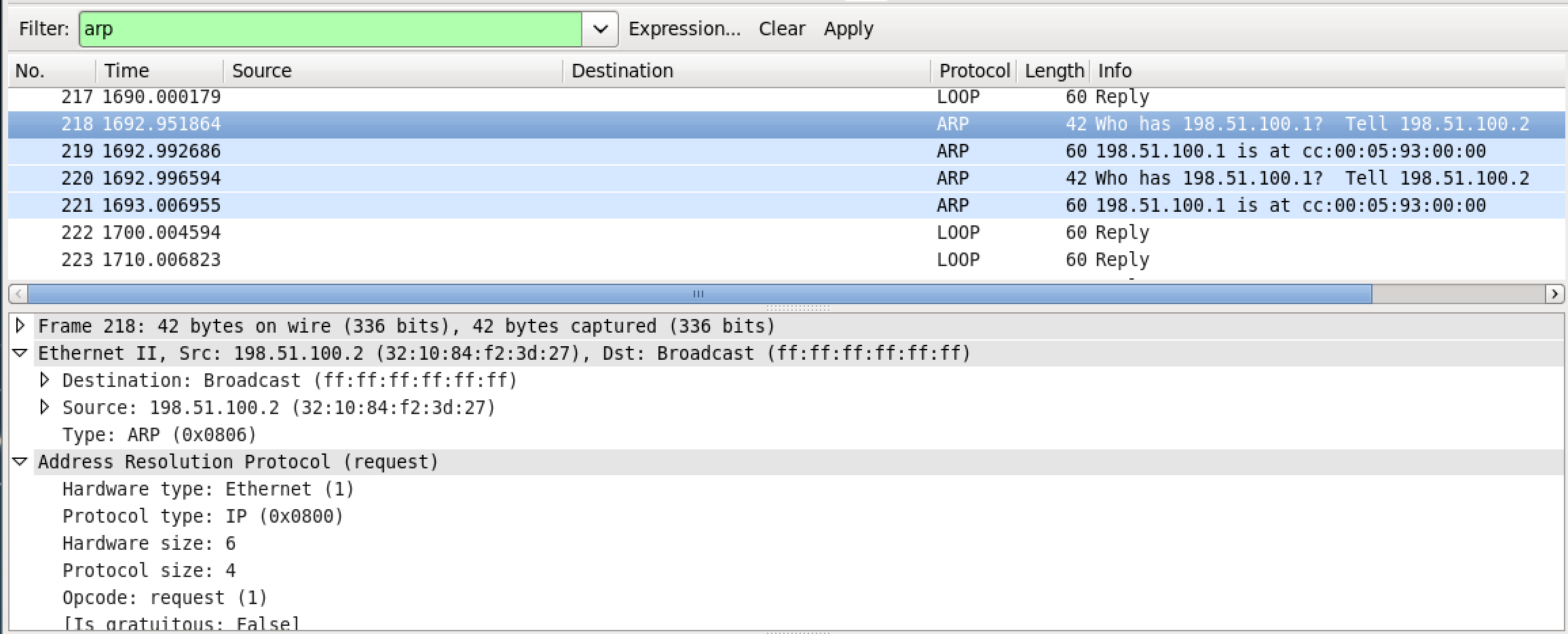


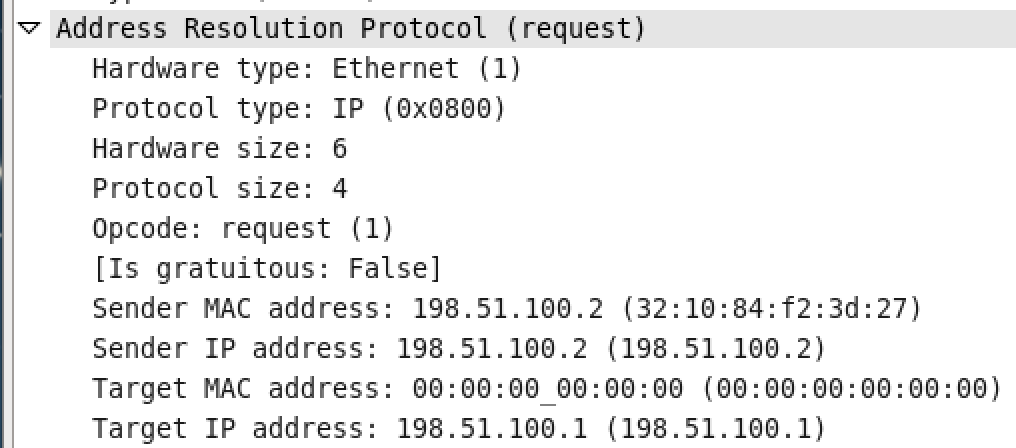


1. Based on your understanding of ARP, answer the following questions **[2 points each]:**

* What filter did you use to only display ARP messages and what are the contents of an ARP message?

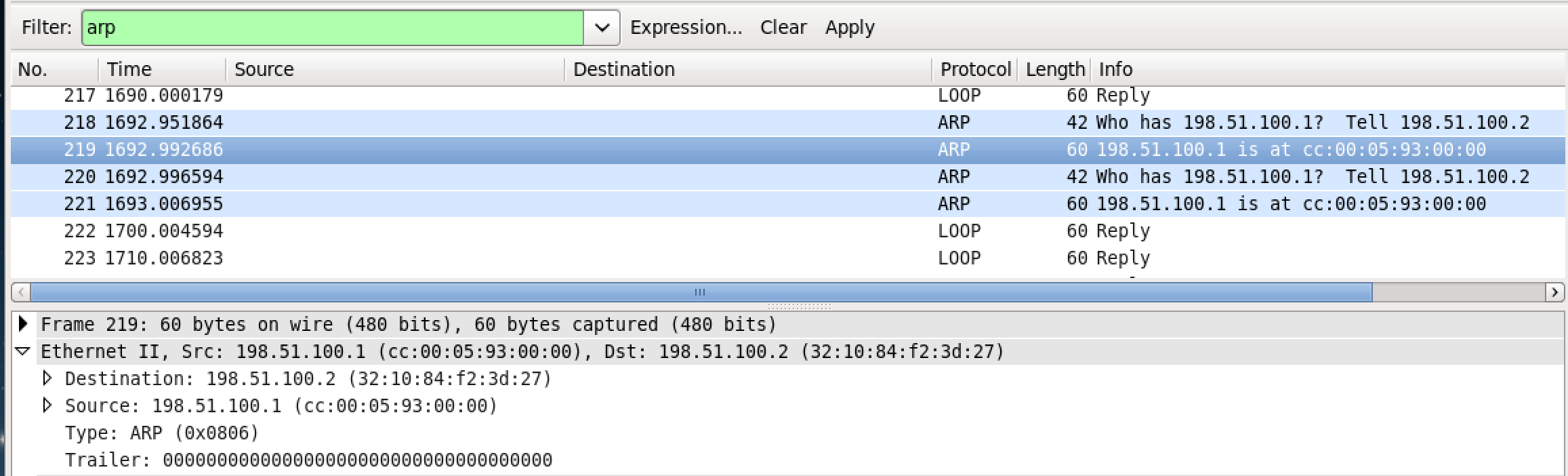
The filter I use in WireShark is arp. The content of the pack in Request is broadcase and src address and MAC address are from C1. But since it’s ARP, so the packet is trying to find target MAC address.

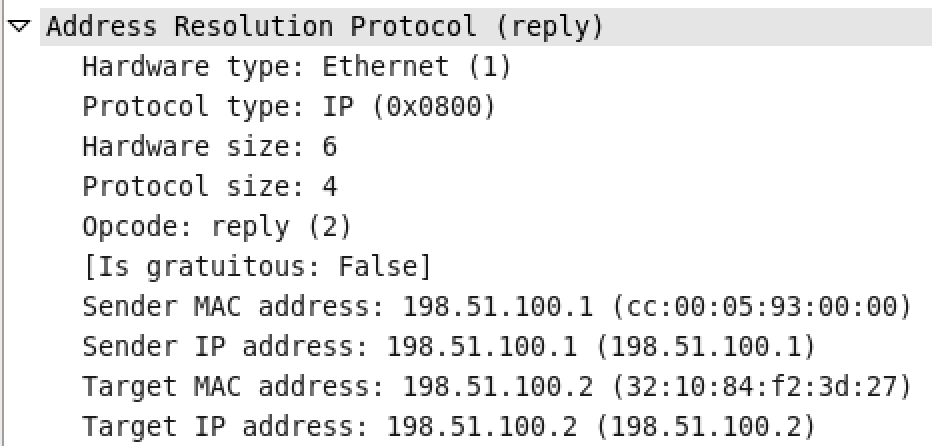




In response:

Target is replying back to the src address with target itself MAC address.





* Which field in an ARP message is used to identify if it is an ARP request or an ARP reply?

You can see in the Request packet, the destination is broadcast (ff:ff:ff:ff:ff:ff). Also, Expand Ethernet II to view Ethernet details, you can see the type field is ARP (0x0806), this means ARP.

In the Response, the destination field is C1’s MAC address. In the source field, this is MAC address of default gateway.

* What is a Gratuitous ARP and why is it used?

A gratuitous ARP is ARP request packet where the source and destination IP are set to the IP of the device issuing the packet, and the MAC is the broadcast address. The following reasons why it is used:

* It will check if there’s IP conflict. A device receives an ARP request, if it matches ARP table, it will know there is a IP conflict
* Gratuitous ARP inform switches of the MAC address of the device on a given switch port, so the switch knows that it should transmit packets and send to that MAC address on that switch port.
* When an IP interface or link goes up every time, the driver for that interface will send a gratuitous ARP to preload the ARP tables of all other local host. Then, a gratuitous ARP will tell us that host just had had a link up event. If we see multiple gratuitous ARPs from the same host, it could be bad Ethernet hardware or cable problems
* Which layer in the OSI model does ARP belong and why?

It belongs to layer 2 because it’s a broadcast and broadcast is sent to layer 2. Normally, ARP does traverse to layer 3.

* What is Proxy ARP and why is it used ?

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. The router accepts responsibility for touting packets to the “real” destination by faking it. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway. [8]

Objective 2: SYN flood using Scapy:

“Bringing down a server” is typically a moment of pride in the world of hackers. SYN flood is one of the popular denial-of-service attacks that targets the end system (especially a server). It is an event where the attacker sends a succession of SYN requests (to which the server responds with a SYN-ACK) with an intent to consume enough resources that will make the server unresponsive to legitimate traffic and eventually bring it down. In this objective you will create a SYN packet and initiate a SYN flood attack using Scapy.

1. Create your own SYN packet using Scapy and display the packet structure. **[10 points]**



1. Initiate a SYN flood attack to the router’s interface from the VM (C1). Show how you initiated the attack through Scapy and show the relevant traffic on Wireshark. **[20 points]**

This is how I run the program, it takes target ip address as argument:

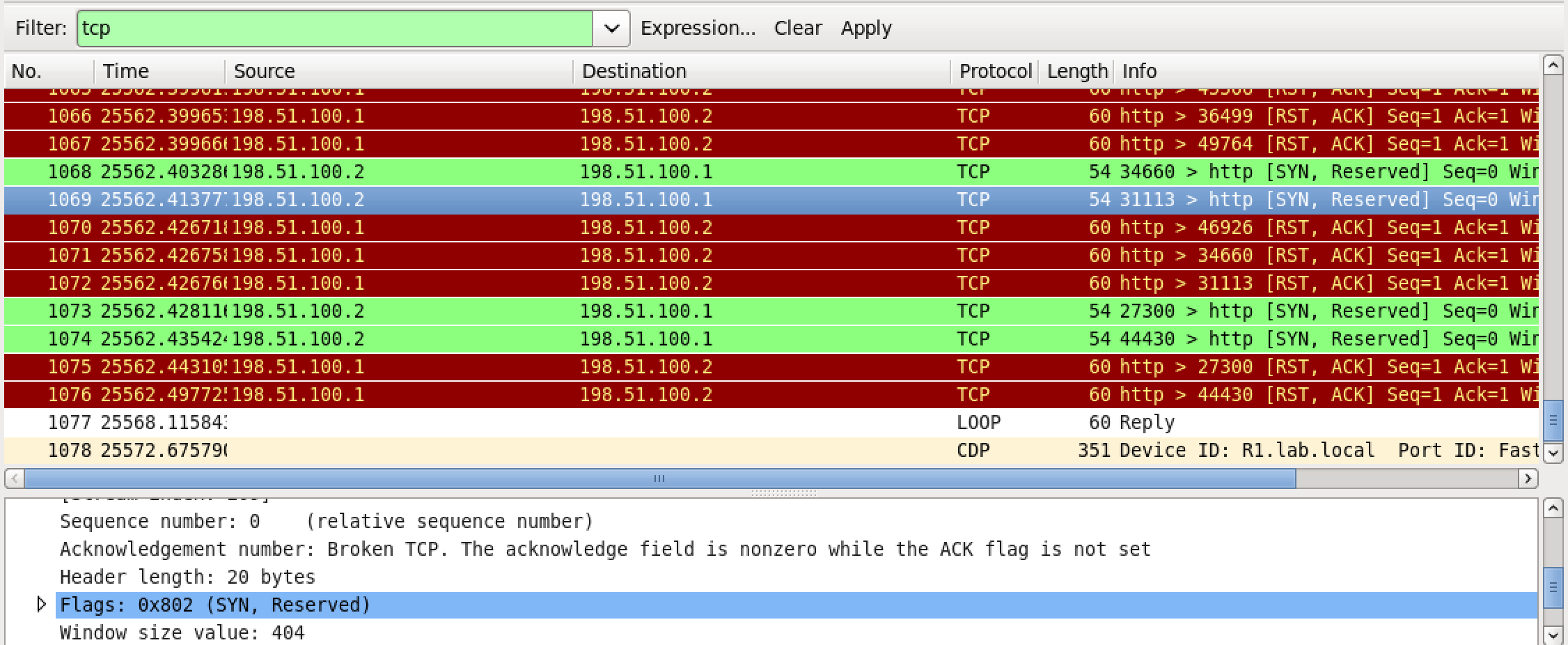


I loop 200 times to send packets to the node with a flags (S = SYN) on port 80. The function fuzz() is able to change any default value that is not to be calculated (like checksums) by an object whose value is random and whose type is adapted to the field. This enables to quickly built fuzzing templates and send them in a loop [1]

﻿ for i in range (0, 200):

message = ( (IP(dst=args.host)) / fuzz(TCP(dport=80,flags='S')) )

send(message)

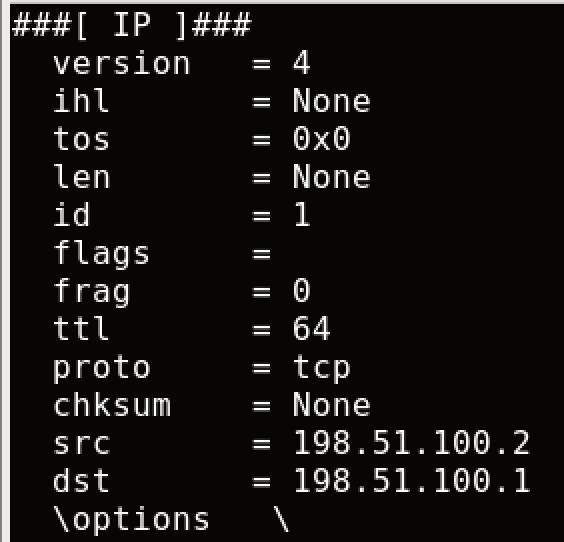


1. Give two ways on how you will prevent such an attack from happening. **[10 points]**

* You can do TCP Intercept feature to prevent TCP SYN flooding attack. This feature will intercept and validate TCP connection requests. When user turn on the intercept mode, the software will intercept SYN packets that match an extended access list from clients to servers. [2]
* Firewall/Proxy: This mechanism spoofs ACKs to the listen in response to observed SYN-ACKs and this prevents the listeners TCBs from staying in the SYN-RECEIVED state, so this can maintain free space in backlog. [3]

Objective 3: Creating your own Telnet packet using Scapy:

1. Create your own Telnet packet using Scapy and display the packet structure. **[10 points]**

****

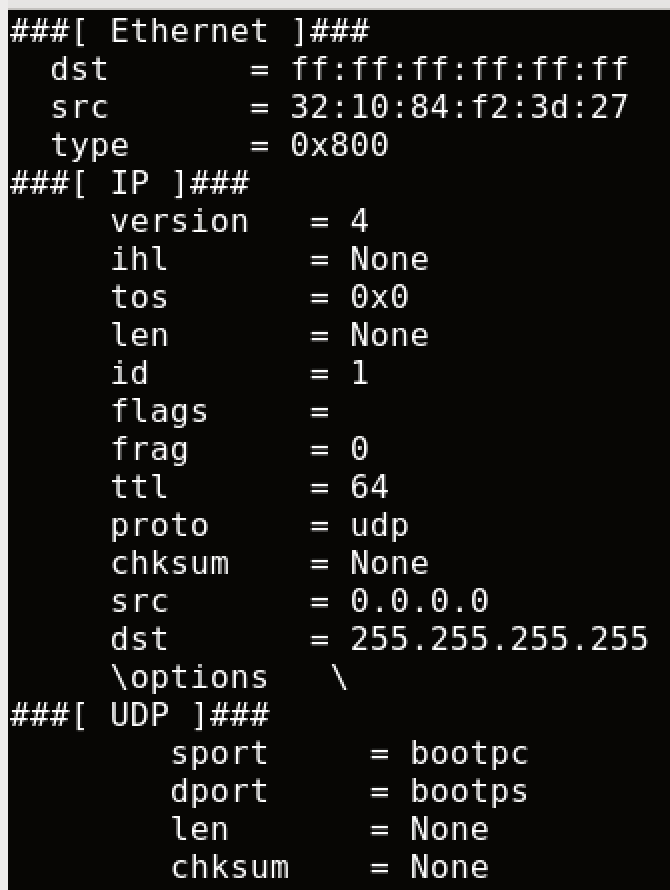
1. Display the Telnet traffic using Wireshark. **[5 points]**

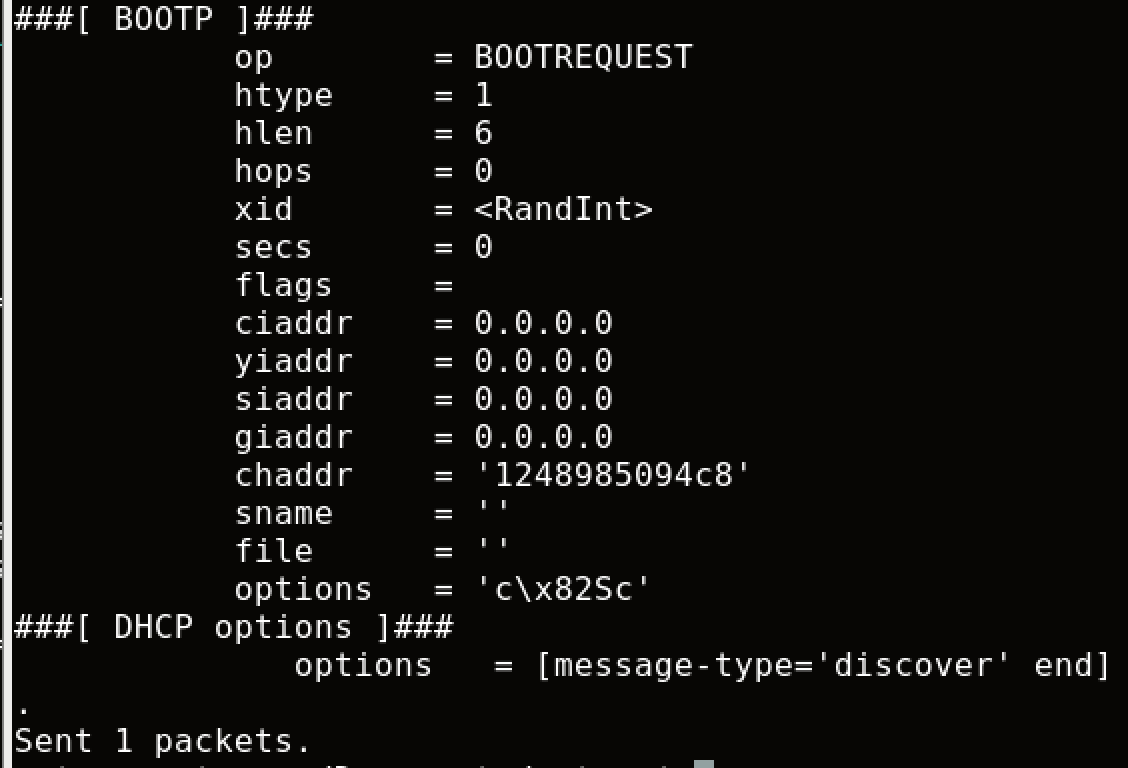


Extra Credit 1 [10 points]

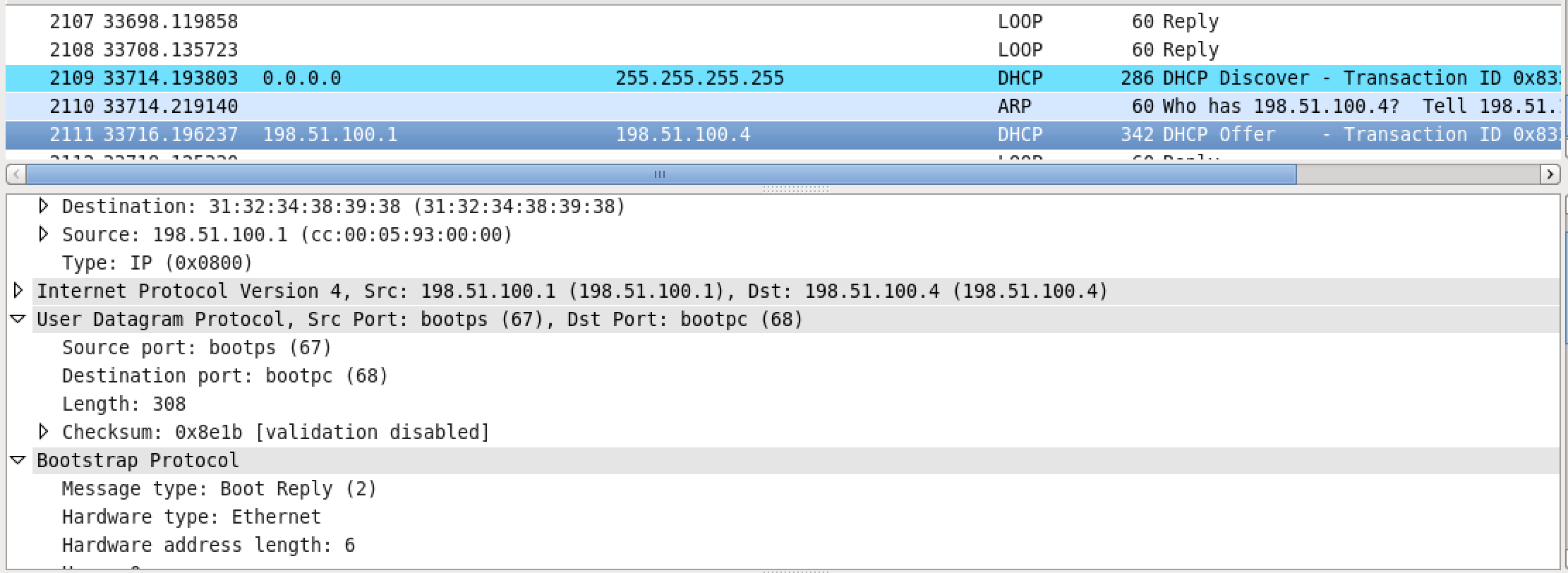
Make R1 as the DHCP server for your VM (C1) as the client.

1. Create your own DHCP discover packet using Scapy and display the packet structure. **[5 points]**

****

****

1. Show the DHCP Server reply packets on Wireshark. **[5 points]**

****

Extra Credit 2 [10 points]

1. Repeat the Scapy Objective 1 (Create an ICMP echo request and ARP frame through Scapy) using IPv6. Answer questions 1 to 4 with respect to IPv6. Paste relevant screenshots. (HINT: Are you sure it is ARP?)

**QUESTIONS: [50 Points]**

1. Explain the difference between stateless and stateful DHCPv6. **[10 points]**

* Stateful in DHCPv6: some system exists that can keep track of information in a log such that certain IP addresses were assigned to certain MAC addresses.
* Stateless in DHCPv6: Instead of keeping track of IP addresses have been assigned, it simply determines what address it should be used on network, and then use DAD (Duplicate Address Detection) to check if it selected address has been already in use.

1. When will you use an IPv6 helper address in a DHCPv6 configuration? Explain briefly how and why you would use an IP helper address. **[10 points]**

There is no broadcast or ipv6 helper address in IPv6, but rather configuration of the IPv6 relay with ‘ipv6 dhcp relay destination’.

We use helper address when the DHCP server is on another subnet. DHCP is not the only critical service that uses broadcasts. In a hierarchical network, clients might not be in the same subnet with key servers. Such remote clients broadcast to locate there servers, but by default, routers do not forward client broadcasts beyond their subnet, then some clients cannot to make connection without services like DHCP. In this case, the network engineer needs to give ip helper-address command feature to relay broadcast requests for these UDP services. [4]

1. Explain the concept of prefix delegation? [ Hints: Delegating Router and Requesting Router] **[10 points]**

Prefix delegation (PD) is considered to be a mechanism that is used to automate the delegation of IPv6 address blocks, and this normally is used by ISPs, to help with the process of delegating IPv6 address blocks to their customer.

Cisco’s version of PD has three types, Customer Edge (CE), Provider Edge (PE), and AAA server. [5]

The CE router which is Requesting Router[RR], is acting like DHCP client at the customer’s premises. Its job is to request IPv6 prefixes (address blocks) from the Provider Edge (PE) router.

The PE router which is Delegating Router (DR) is acting like DHCP server at provider premises. Its responsibilities of validating the authenticity and the profile of the RR with the AAA server, and also places a route into the ISP’s routing system on the behalf of the RR for the delegated prefix.

1. Explain the significance of DUID? **[10 points]**

Each operation in DHCP operation, the client and server have DHCP unique identifier (DUID). Client uses DUID to identify a server in messages where a server needs to be identified. DHCP servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with client. [6]

1. Briefly describe how DHCPv6 prefix delegation can induce security risks in the network? State ways to mitigate these risks. **[10 points]**

Because SLAAK doesn’t do everything that a ISP want, the provider can elect to use DHCPv6. The service provider’s layer 3 edge router can send a RA message to notice customers that DHCPv6 is in use, then the RA sends the A/M/O buts to tell the node that DHCPv6 is available. In this case, there can still be concern that the RA message could be spoofed by an attacker. [7]

User could use a RADIUS server, which is a distributed client/server that secure networks against unauthorized access to authenticate the prefix delegation.

**REFLECTION [ 5 Points]:**

1. What did you learn from this lab and how would you incorporate this in a production network setting? **[5 points]**

I have learned a lot from automating the telnet, configuring, and doing some simple attacks using Python script. I can feel automation for Networking will be a big future. I will definitely secure and configure some more protections for my routers in work. There are many ways to attack and as network engineer, we need to think 3 steps ahead of attacks.

# Total Score = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/295 + (20 Bonus)

References:

1. <https://scapy.readthedocs.io/en/latest/usage.html>

2. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_dos_atprvn/configuration/15-mt/sec-data-dos-atprvn-15-mt-book/sec-cfg-tcp-intercpt.html>

3. <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-34/syn-flooding-attacks.html>

4. <http://www.ciscopress.com/articles/article.asp?p=330807&seqNum=9>

5. <http://www.techtutorials.net/articles/ipv6_training_cisco_what_is_prefix_delegation_.html>

6. <https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/dhcp-unique-id-servers-clients-overview.html>

7. <http://www.ciscopress.com/articles/article.asp?p=1312796&seqNum=6>

8. https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/13718-5.html