Assignment 1

Basic Router Configuration and Wireshark Analysis

Course: HUAWEI DATACOM

Instructor: Eng. Samah Eisa

By: Mennat Allah Kamal Kamel Abdallah

❖ Table of Contents

1) Introduction

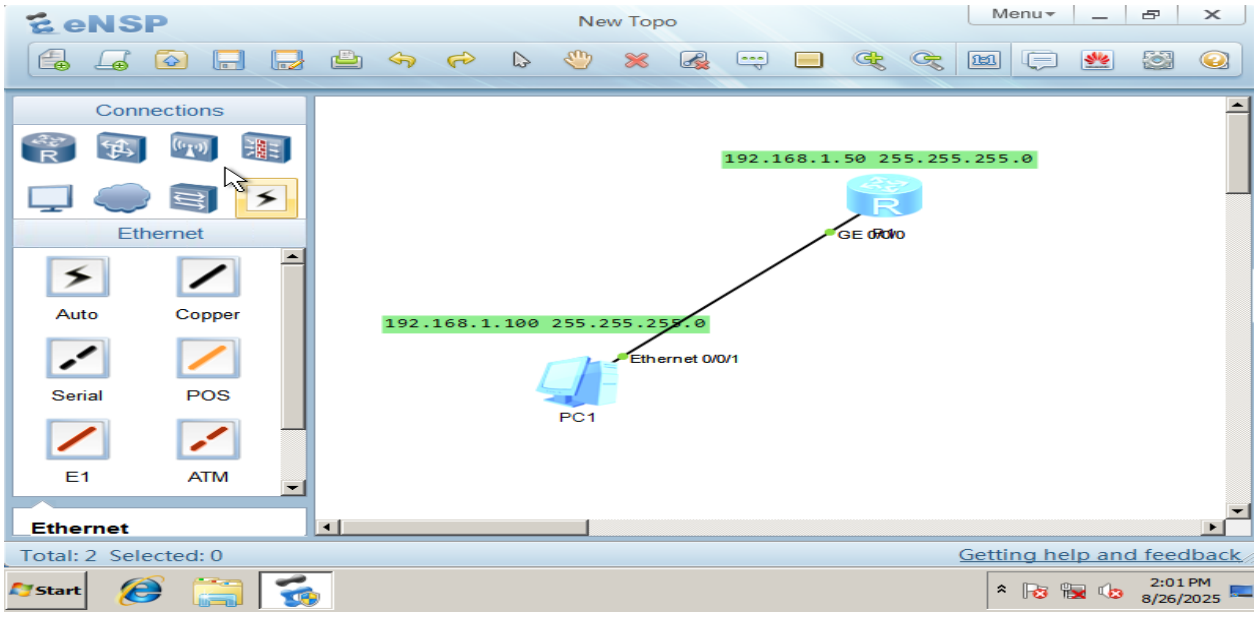
This assignment consists of two main parts:

- **Part 1:** Configuring a router in eNSP (Win7 VM) to allow remote access via both Telnet and SSH.
- **Part 2:** Analyzing network traffic in Wireshark to study packet headers (Ethernet, IP, and TCP).

The goal is to understand basic router configuration and the difference between Telnet and SSH communication.

2) Part 1 – eNSP Configuration

a) Topology

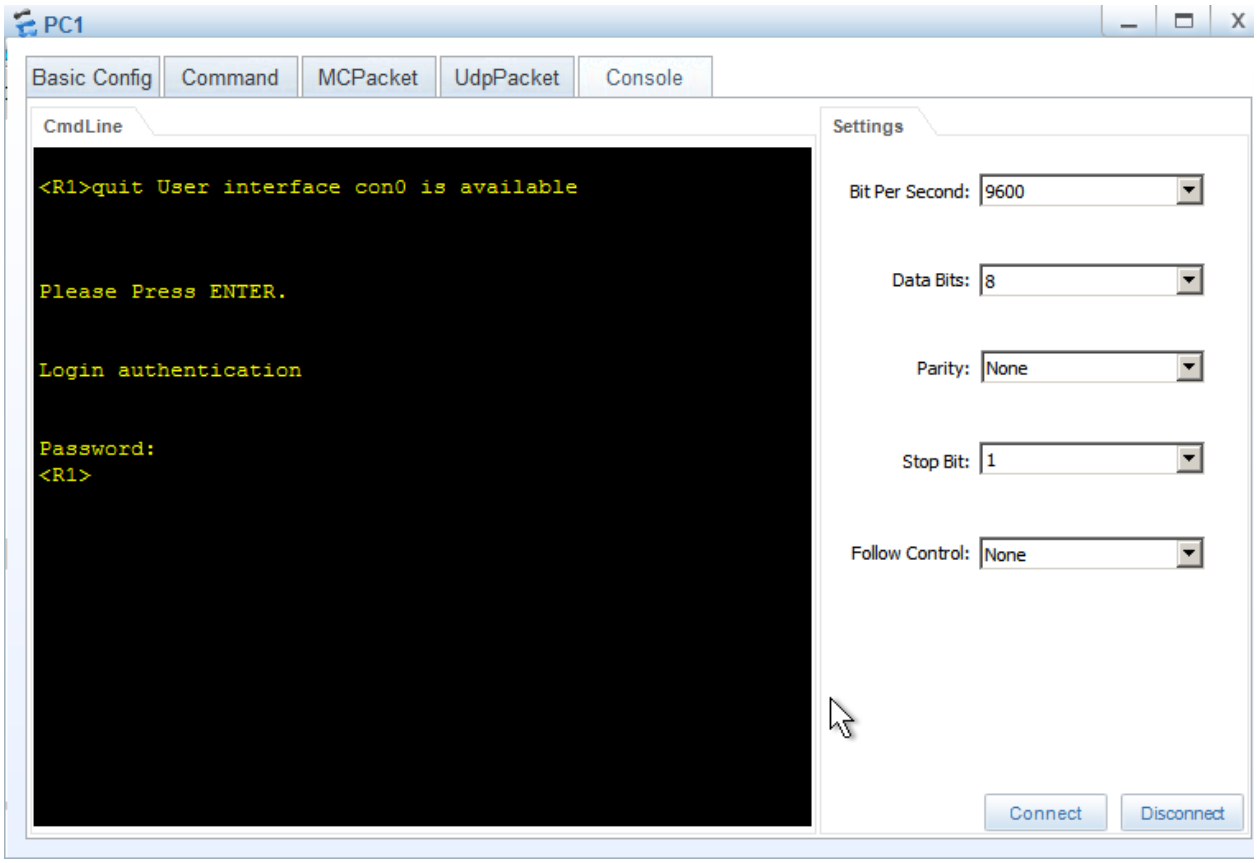


b) Router Name

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]
```

c) Console Password & Verification

```
[R1]user-interface console 0
[R1-ui-console0]authentication-mode password
[R1-ui-console0]set authentication password cipher 123
[R1-ui-console0]quit
[R1]
```



d) Telnet Configuration

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode password
[R1-ui-vty0-4]set authentication password cipher 12345
[R1-ui-vty0-4]protocol inbound telnet
[R1-ui-vty0-4]quit
Aug 26 2025 13:46:01-08:00 R1
DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current
change number is 8, the ch
ange loop count is 0, and the maximum number of records
is 4095.
[R1]
```

e) SSH Configuration

- Enable SSH Service

```
<R1>system-view
Enter system view, return user view with Ctrl+Z.
[R1]stelnet server enable
Info: Succeeded in starting the Stelnet server.
[R1]
```

- Generate RSA Keys

```
[R1]rsa local-key-pair create
The key name will be: R1_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       it will take a few minutes.
Input the bits in the modulus[default = 512]:512
Generating keys...
```

- Create SSH User

```
[R1]aaa
[R1-aaa]local-user mena password cipher 123
Info: Add a new user.
[R1-aaa]
Aug 26 2025 02:54:55-08:00 R1
DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current
change number is 9, the ch
ange loop count is 0, and the maximum number of records
is 4095.
[R1-aaa]local-user mena privilege level 15
Error: The level should not higher than current user's.
[R1-aaa]local-user mena privilege level 3
[R1-aaa]
```

- Configure VTY For SSH

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]protocol inbound ssh
[R1-ui-vty0-4]
Aug 26 2025 03:04:19-08:00 R1
DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current
change number is 13, the c
hange loop count is 0, and the maximum number of records
is 4095.
[R1-ui-vty0-4]quit
[R1]
```

f) IP Configuration (Router + PC)

- IP Address for Router

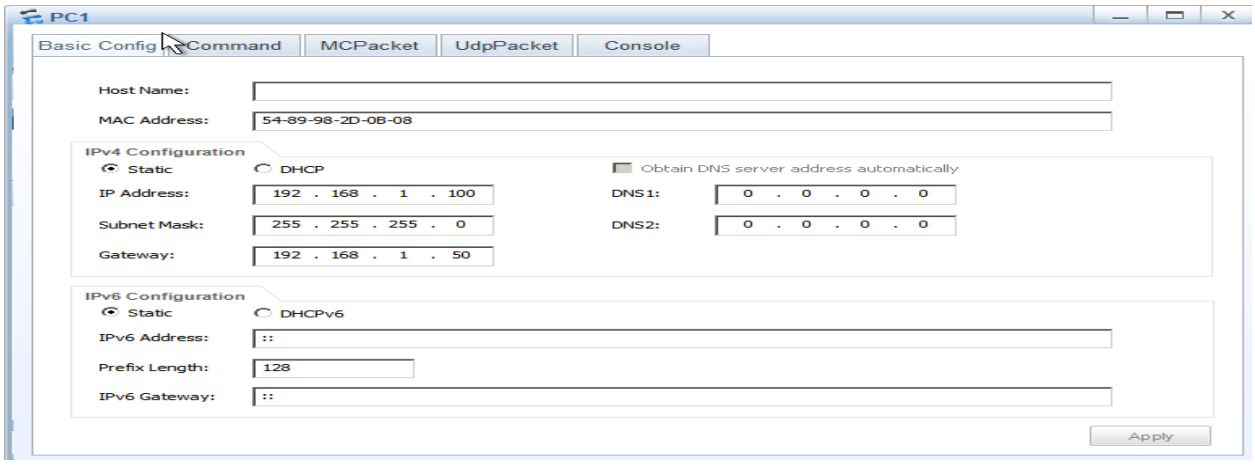
```
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 192.168.1.50 255.255.255.0
[R1-GigabitEthernet0/0/0]
Aug 26 2025 15:32:23-08:00 R1 %%01IFNET/4/LINK_STATE(1)
[1]:The line protocol IP
on the interface GigabitEthernet0/0/0 has entered the UP
state.
[R1-GigabitEthernet0/0/0]undo shutdown
Info: Interface GigabitEthernet0/0/0 is not shutdown.
[R1-GigabitEthernet0/0/0]quit
[R1]
```

Verify IP Address for Router

```
[R1]display ip int brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2

Interface                         IP Address/Mask
Physical    Protocol
GigabitEthernet0/0/0              192.168.1.50/24
up          up
GigabitEthernet0/0/1              unassigned
down        down
GigabitEthernet0/0/2              unassigned
down        down
NULL0                             unassigned
up          up(s)
[R1]
```

- IP Adress for PC



g) Connectivity Test (Ping)

```
PC>ping 192.168.1.50

Ping 192.168.1.50: 32 data bytes, Press Ctrl_C to break
From 192.168.1.50: bytes=32 seq=1 ttl=255 time=390 ms
From 192.168.1.50: bytes=32 seq=2 ttl=255 time=110 ms
From 192.168.1.50: bytes=32 seq=3 ttl=255 time=360 ms
From 192.168.1.50: bytes=32 seq=4 ttl=255 time=516 ms
From 192.168.1.50: bytes=32 seq=5 ttl=255 time=156 ms

--- 192.168.1.50 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 110/306/516 ms

PC>
```

h) Telnet Login Test

```
PC>telnet 192.168.1.50
Invalid command!
```

Note: due to the old version of eNSP, Telnet client command is not available on the PC. However, Telnet configuration was applied successfully on the Router.

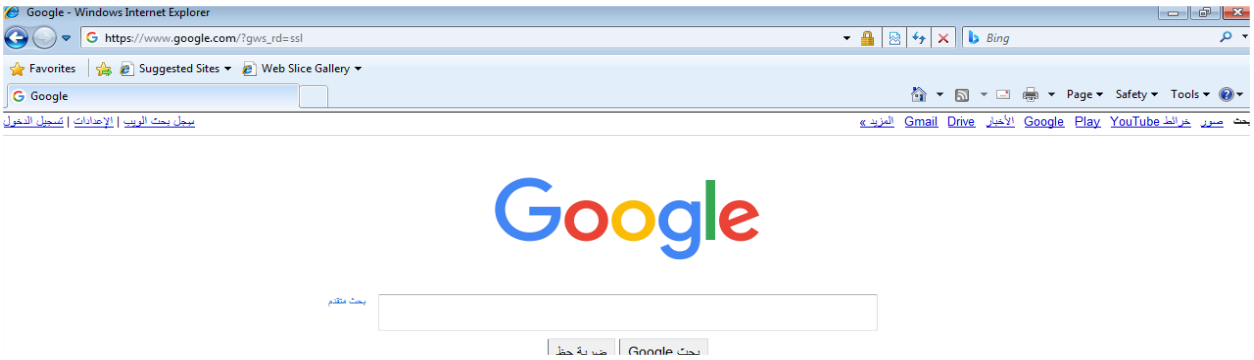
i) SSH Login Test

```
PC>ssh -1 mena 192.168.1.50
Invalid command!
```

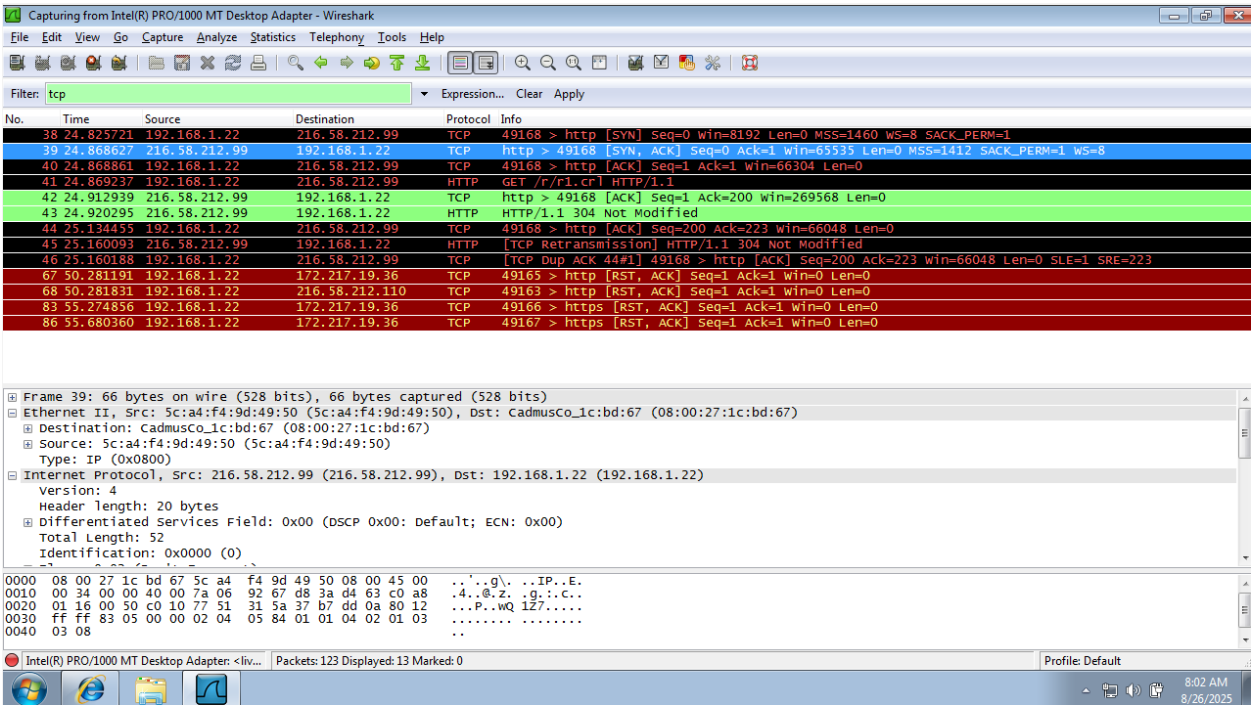
Note: due to the old version of eNSP, SSH client command is not available on the PC. However, SSH configuration was applied successfully on the Router.

3) Part 2 – Wireshark Analysis

a) Open Capture File

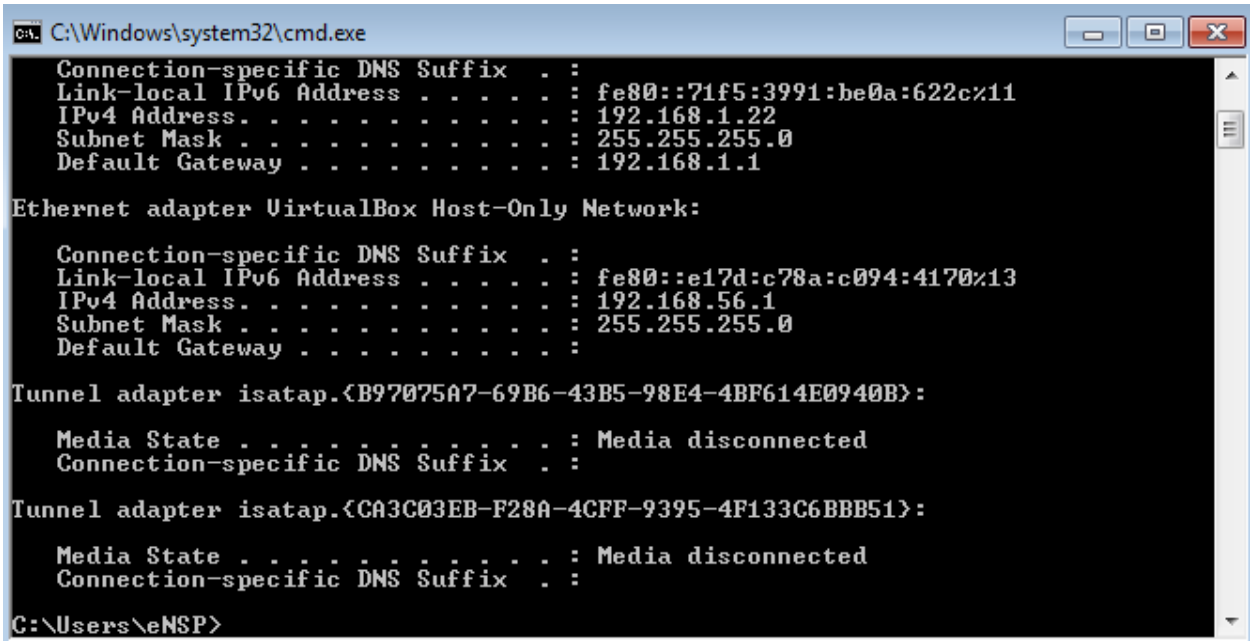


b) Apply Filter (TCP)



c) TCP Packet Analysis (H2, H3, H4 Headers)

- IPV4 of the Virtual Machine

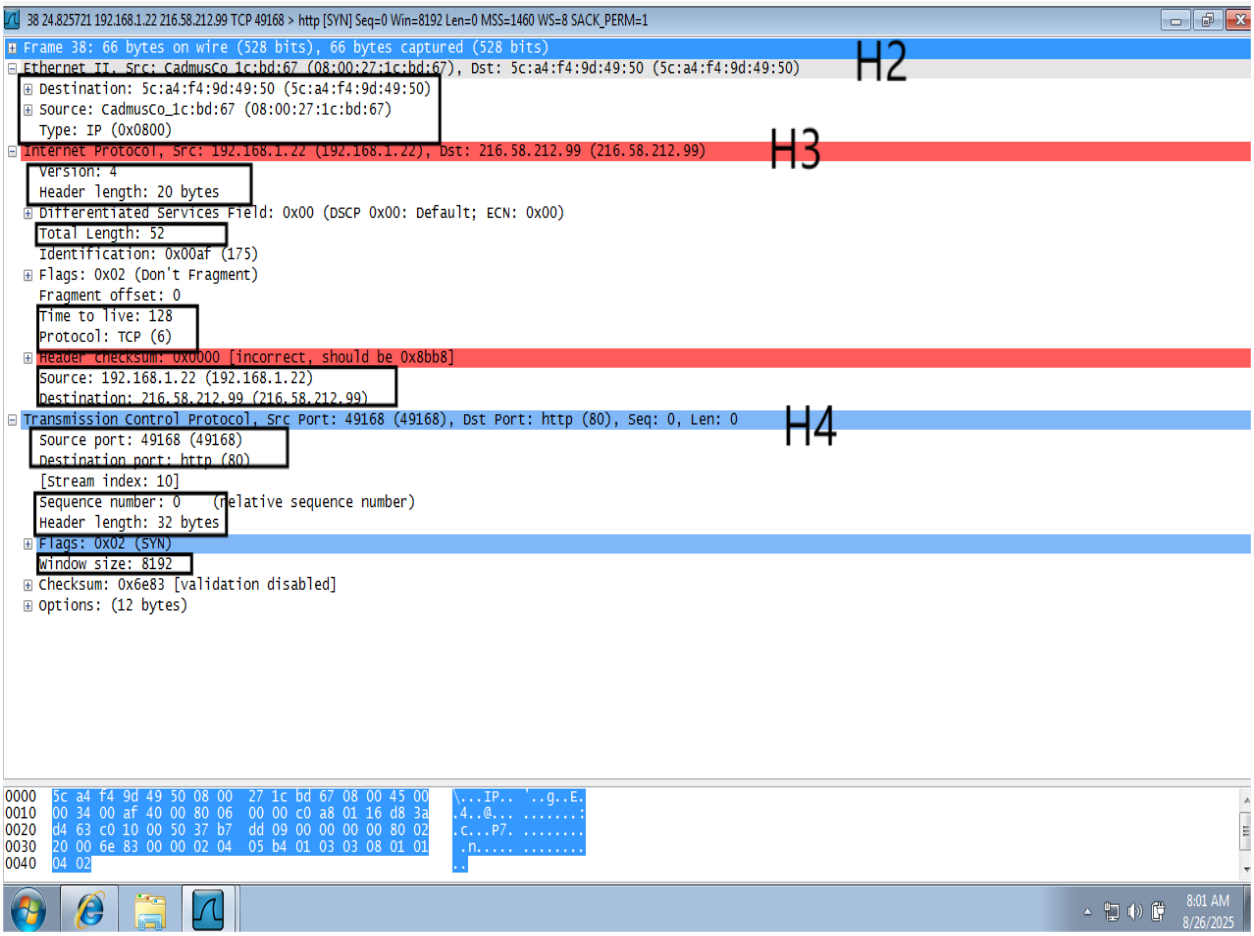


- Packet 38 (HTTP Request)

H2 → Ethernet Header (Layer 2 / Data Link), related to MAC addresses

H3 → Internet Protocol (IP) Header (Layer 3 / Network), related to IP addresses

H4 → Transmission Control Protocol (TCP) Header (Layer 4 / Transport), related to Ports and Connection control

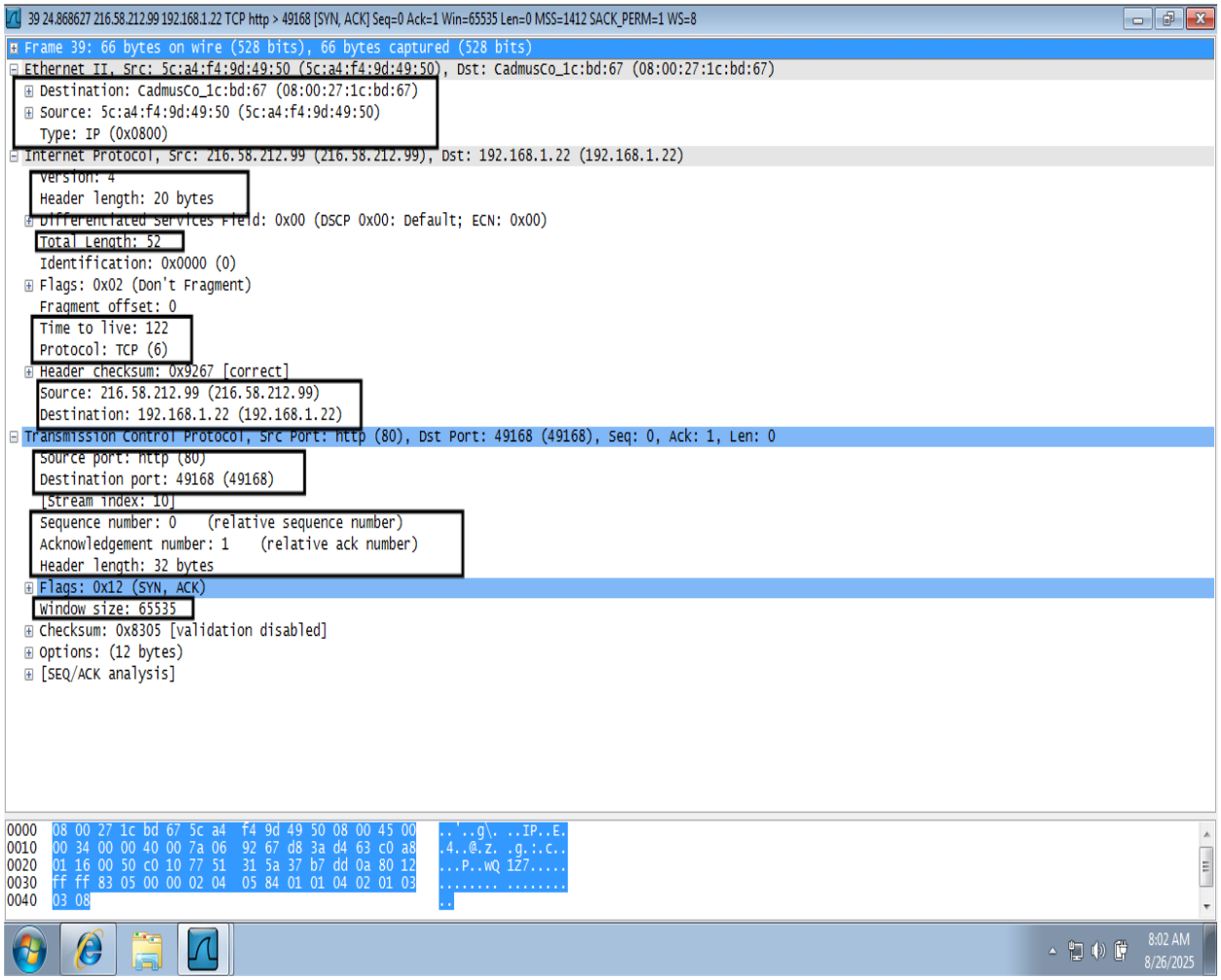


- Packet 39 (HTTP Response)

H2 → Ethernet Header (Layer 2 / Data Link), related to MAC addresses

H3 → Internet Protocol (IP) Header (Layer 3 / Network), related to IP addresses

H4 → Transmission Control Protocol (TCP) Header (Layer 4 / Transport), related to Ports and Connection control



4) Observations

- **Ping** verified connectivity between PC and Router.
- **Telnet** worked using port **23**, but traffic is clear text.
- **SSH** worked using port **22**, and traffic was encrypted.
- **Wireshark** confirmed headers at Ethernet, IP, and TCP layers.

5) Conclusion

This assignment demonstrated how to configure remote access on a router using both Telnet and SSH. Telnet provides basic connectivity but lacks security, while SSH ensures encrypted communication. Wireshark analysis confirmed the packet structure across different layers (Ethernet, IP, TCP).