



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

2) Part 1 – eNSP Configuration

- a) Topology
- b) Router Name
- c) Console Password & Verification
- d) Telnet Configuration
- e) SSH Configuration
- f) IP Configuration (Router + PC)
- g) Connectivity Test (Ping)
- h) Telnet Login Test
- i) SSH Login Test

3) Part 2 – Wireshark Analysis

- a) Open Capture File
- b) Apply Filter (TCP)
- c) TCP Packet Analysis (H2, H3, H4 Headers)

4) Observations

5) Conclusion

1) Introduction

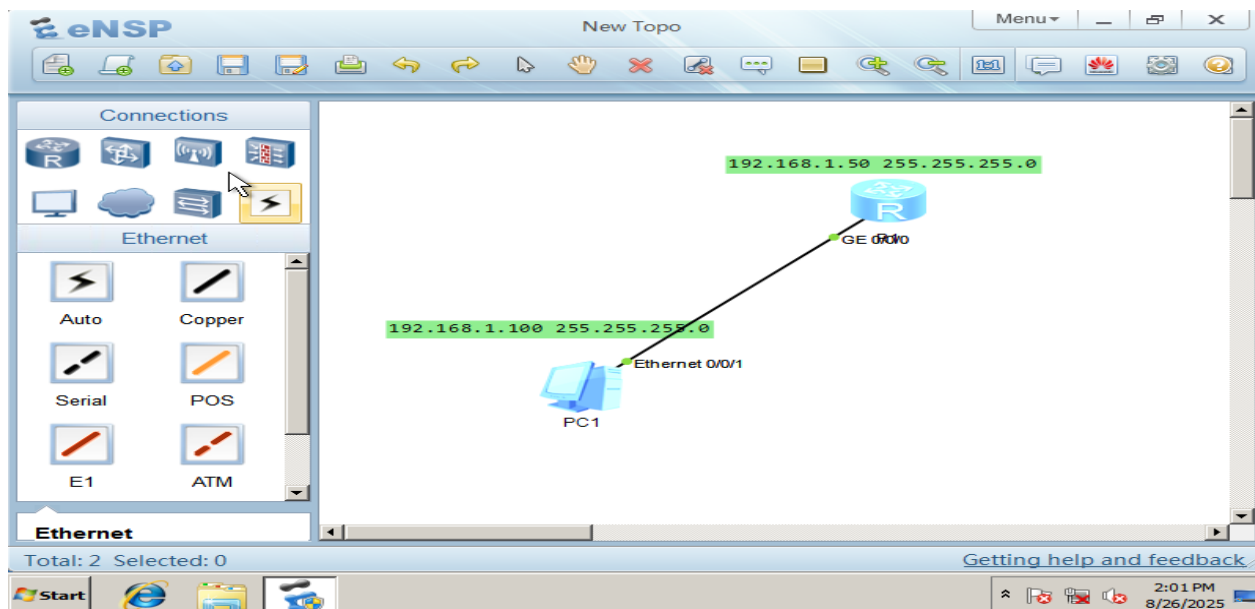
This assignment consists of two main parts:

- **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

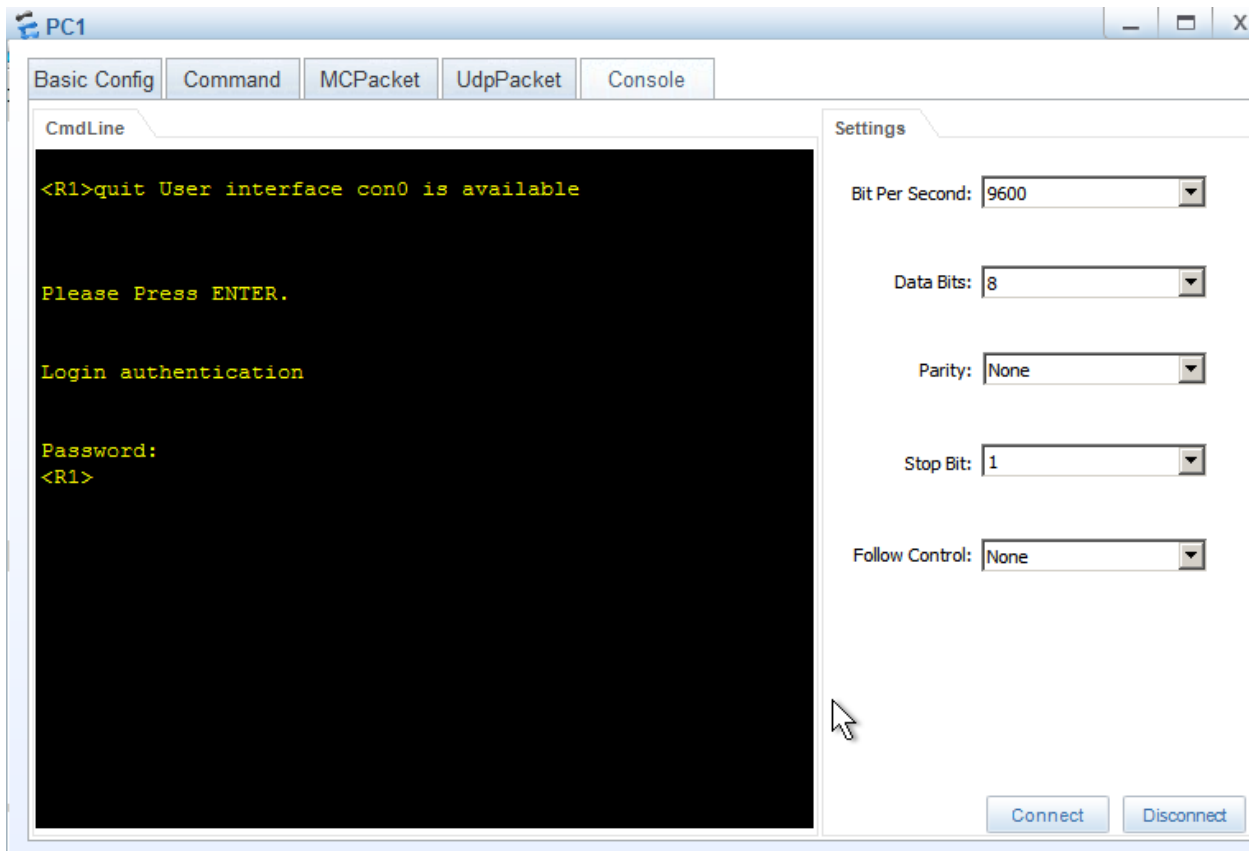


b) Router Name

```
<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
GigabitEthernet0/0/1      unassigned
down
GigabitEthernet0/0/2      unassigned
down
NULL0                    unassigned
up                        up(s)
[R1]|
```

- IP Address for PC

The screenshot shows the 'PC1' configuration window with the 'Basic Config' tab selected. The 'Host Name' field is empty. The 'MAC Address' field contains '54-89-98-2D-08-08'. Under 'IPv4 Configuration', the 'Static' radio button is selected. The 'IP Address' field contains '192 . 168 . 1 . 100', the 'Subnet Mask' field contains '255 . 255 . 255 . 0', and the 'Gateway' field contains '192 . 168 . 1 . 50'. The 'DHCP' radio button is unselected. The 'Obtain DNS server address automatically' checkbox is unchecked. The 'DNS1' field contains '0 . 0 . 0 . 0' and the 'DNS2' field contains '0 . 0 . 0 . 0'. Under 'IPv6 Configuration', the 'Static' radio button is selected. The 'IPv6 Address' field contains '::', the 'Prefix Length' field contains '128', and the 'IPv6 Gateway' field contains '::'. The 'DHCPv6' radio button is unselected. An 'Apply' button is located at the bottom right of the window.

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.

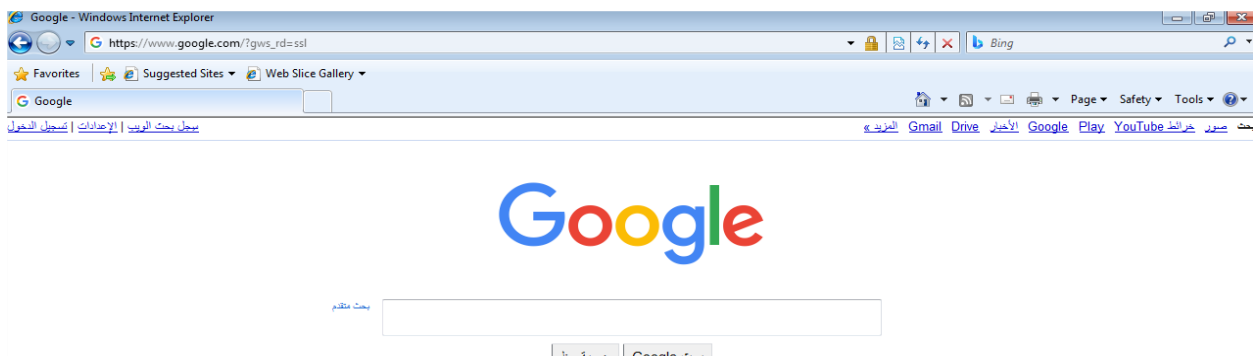
i) SSH Login Test

```
PC>ssh -l 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



Wireshark packet capture showing a series of HTTP and TCP packets. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Info. The middle pane shows the details of the selected packet (Frame 39), including Ethernet II, Internet Protocol, and Hypertext Transfer Protocol fields. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
38	24.825721	192.168.1.22	216.58.212.99	TCP	49168 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 SACK_PERM=1
39	24.868627	216.58.212.99	192.168.1.22	TCP	http > 49168 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1412 SACK_PERM=1 WS=8
40	24.868861	192.168.1.22	216.58.212.99	TCP	49168 > http [ACK] Seq=1 Ack=1 win=66304 Len=0
41	24.869237	192.168.1.22	216.58.212.99	HTTP	GET /r/r1.cr/ HTTP/1.1
42	24.912939	216.58.212.99	192.168.1.22	TCP	http > 49168 [ACK] Seq=1 Ack=200 win=269568 Len=0
43	24.920295	216.58.212.99	192.168.1.22	HTTP	HTTP/1.1 304 Not Modified
44	25.134455	192.168.1.22	216.58.212.99	TCP	49168 > http [ACK] Seq=200 Ack=223 win=66048 Len=0
45	25.160093	216.58.212.99	192.168.1.22	HTTP	[TCP Retransmission] HTTP/1.1 304 Not Modified
46	25.160188	192.168.1.22	216.58.212.99	TCP	[TCP Dup ACK 44#1] 49168 > http [ACK] Seq=200 Ack=223 win=66048 Len=0 SLE=1 SRE=223
67	50.281191	192.168.1.22	172.217.19.36	TCP	49165 > http [RST, ACK] Seq=1 Ack=1 win=0 Len=0
68	50.281831	192.168.1.22	172.217.19.36	TCP	49163 > http [RST, ACK] Seq=1 Ack=1 win=0 Len=0
83	55.274856	192.168.1.22	172.217.19.36	TCP	49166 > https [RST, ACK] Seq=1 Ack=1 win=0 Len=0
86	55.680360	192.168.1.22	172.217.19.36	TCP	49167 > https [RST, ACK] Seq=1 Ack=1 win=0 Len=0

Frame 39: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: 5c:a4:f4:9d:49:50 (5c:a4:f4:9d:49:50), Dst: cadmusco_1c:bd:67 (08:00:27:1c:bd:67)
 Destination: cadmusco_1c:bd:67 (08:00:27:1c:bd:67)
 Source: 5c:a4:f4:9d:49:50 (5c:a4:f4:9d:49:50)
 Type: IP (0x0800)
 Internet Protocol, Src: 216.58.212.99 (216.58.212.99), Dst: 192.168.1.22 (192.168.1.22)
 Version: 4
 Header Length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total Length: 52
 Identification: 0x0000 (0)

0000 08 00 27 1c bd 67 5c a4 f4 9d 49 50 08 00 45 00 ..g...IP..E.
 0010 00 34 00 00 40 07 f4 06 92 67 08 3a 04 63 c0 a8 .4..@.Z...g...
 0020 01 16 00 50 c0 10 77 51 31 5a 37 ff dd 80 12P..WQ.....
 0030 ff ff 83 05 00 00 02 04 05 84 01 01 04 02 01 03
 0040 03 08 ..

- **IPV4 of the Virtual Machine**

```
C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::71f5:3991:be0a:622c%11
IPv4 Address. . . . . : 192.168.1.22
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::e17d:c78a:c094:4170%13
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Tunnel adapter isatap.{B97075A7-69B6-43B5-98E4-4BF614E0940B}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

Tunnel adapter isatap.{CA3C03EB-F28A-4CFF-9395-4F133C6BBB51}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

C:\Users\enSP>
```

- Packet 38 (HTTP Request)

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

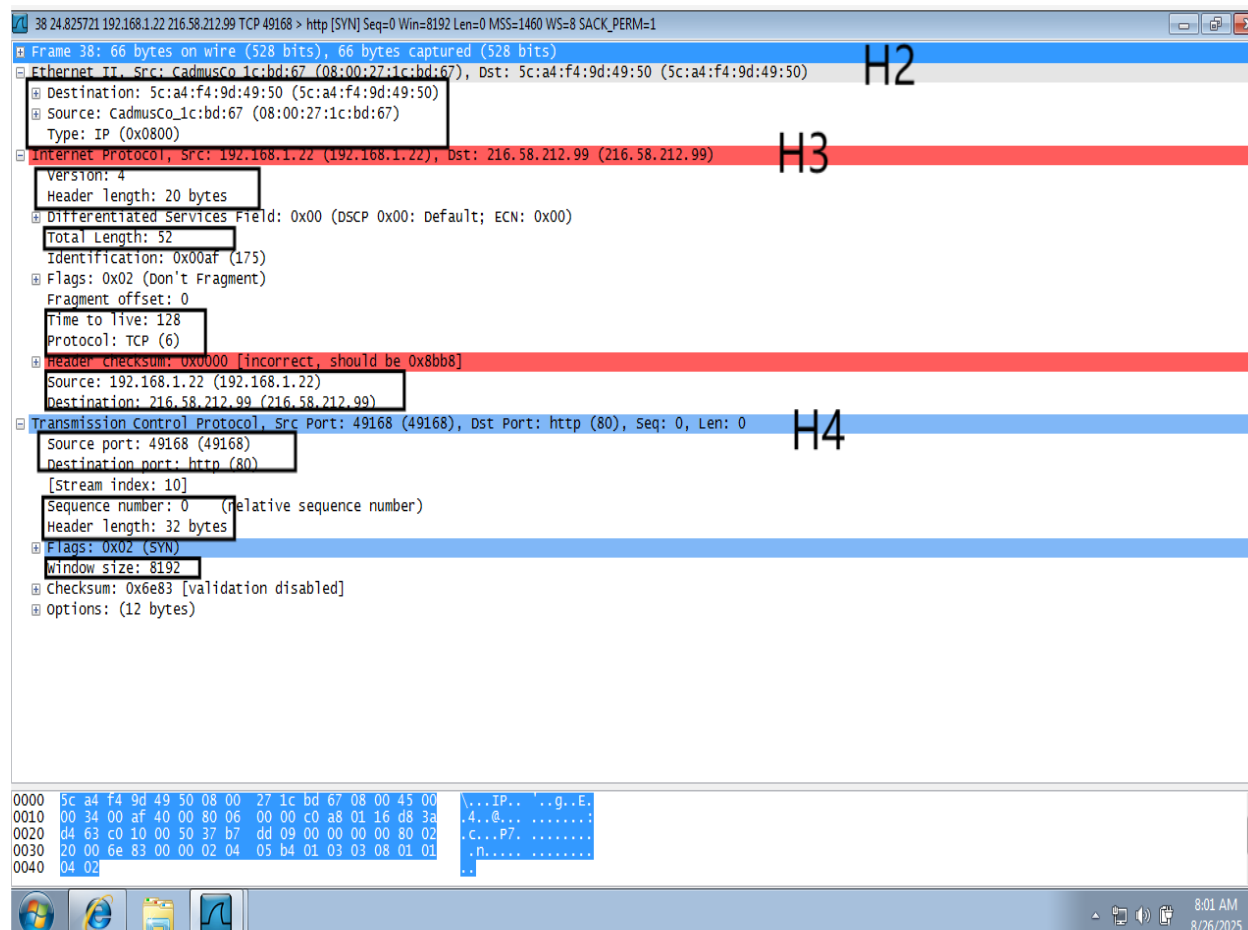
addresses

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)

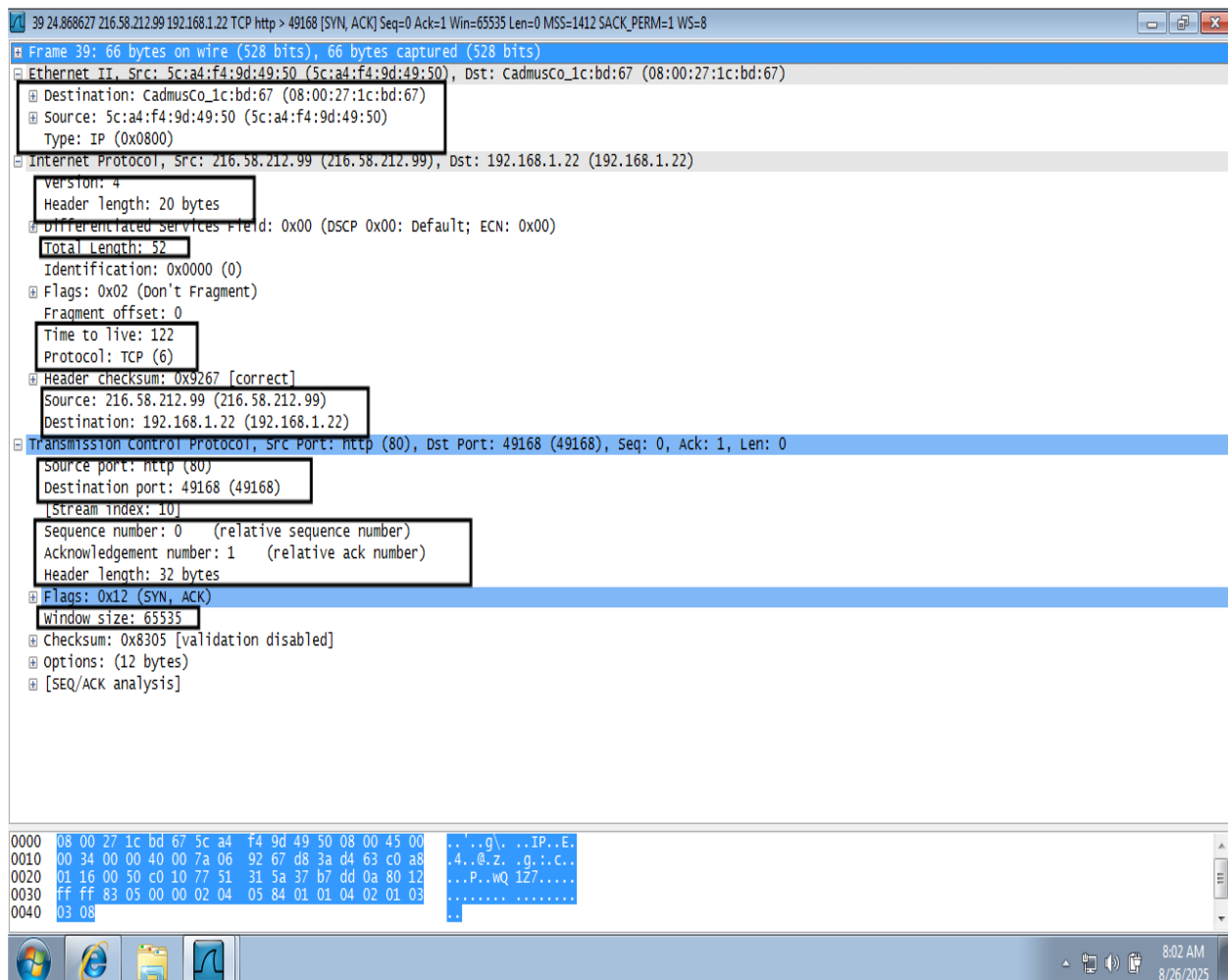
H2 → Ethernet Header (Layer 2 / Data Link), related to MAC

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).