**Lab - Using Wireshark to Examine Ethernet Frames**

# Mininet Topology showing two local area networks. The 172.16.0.0/12 has one workstation directly attached. The 10.0.0.0/24 network has three workstations attached via a switch. Instructions

## Examine the Header Fields in an Ethernet II Frame

### Review the Ethernet II header field descriptions and lengths.

| Preamble | Destination Address | Source Address | Frame Type | Data | FCS |
| --- | --- | --- | --- | --- | --- |
| 8 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 46 – 1500 Bytes | 4 Bytes |

### Examine Ethernet frames in a Wireshark capture.

### Examine the Ethernet II header contents of an ARP request.

| Field | Value | Description |
| --- | --- | --- |
| Preamble | Not shown in capture | This field contains synchronizing bits, processed by the NIC hardware. |
| Destination Address  Source Address | Broadcast (ff:ff:ff:ff:ff:ff)  IntelCor\_62:62:6d  (f4:8c:50:62:62:6d) | Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, 0-9,A-F. A common format is 12:34:56:78:9A:BC.  The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC.  The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast. |
| Frame Type | 0x0806 | For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are:  Value Description  0x0800 IPv4 Protocol  0x0806 Address resolution protocol (ARP) |
| Data | ARP | Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes. |
| FCS | Not shown in capture | Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending machine, encompassing frame addresses, type, and data field. It is verified by the receiver. |

What is significant about the contents of the destination address field?

All the hosts in the network will receive the broadcast frame. The host IP with IP 192.168.1.1 (default gateway) will send a reply to the source. This reply will contain the MAC address of the NIC on the default gateway’s interface.

Why does the PC send out a broadcast ARP prior to sending the first ping request?

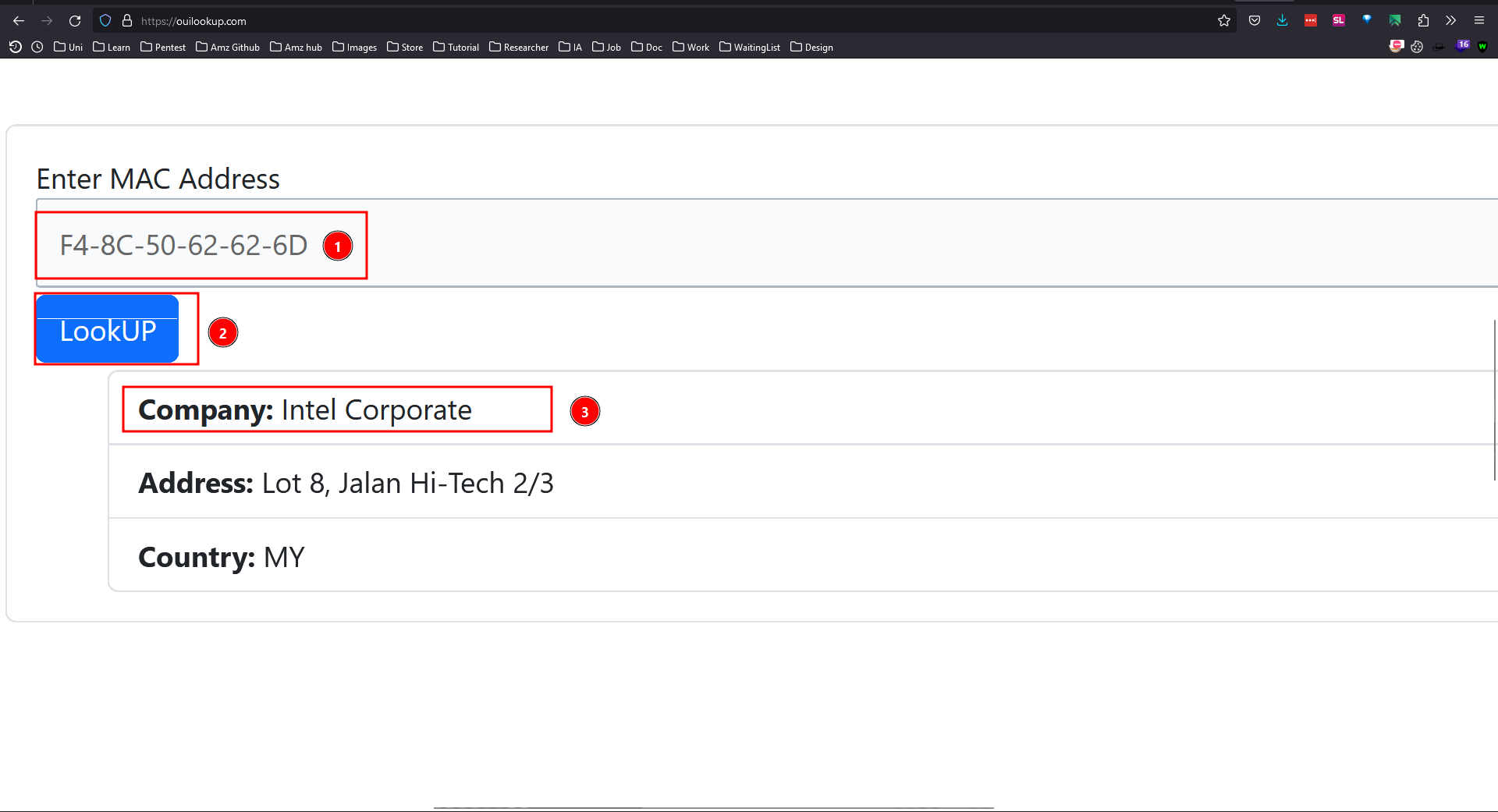
The PC can not send a ping request if it do not know the destination MAC address.

What is the MAC address of the source in the first frame?

F4-8C-50-62-62-6D

What is the Vendor ID (OUI) of the Source’s NIC?

Intel Corporate



What portion of the MAC address is the OUI?

F4-8C-50

What is the Source’s NIC serial number?

62-62-6D

## Use Wireshark to Capture and Analyze Ethernet Frames

### Examine the network configuration of H3.

* + - 1. Start and log into your CyberOps Workstation VM using the following credentials:
      2. Open a terminal emulator to start mininet and enter the following command at the prompt. When prompted, enter **cyberops** as the password.

A screenshot of a computer

Description automatically generated

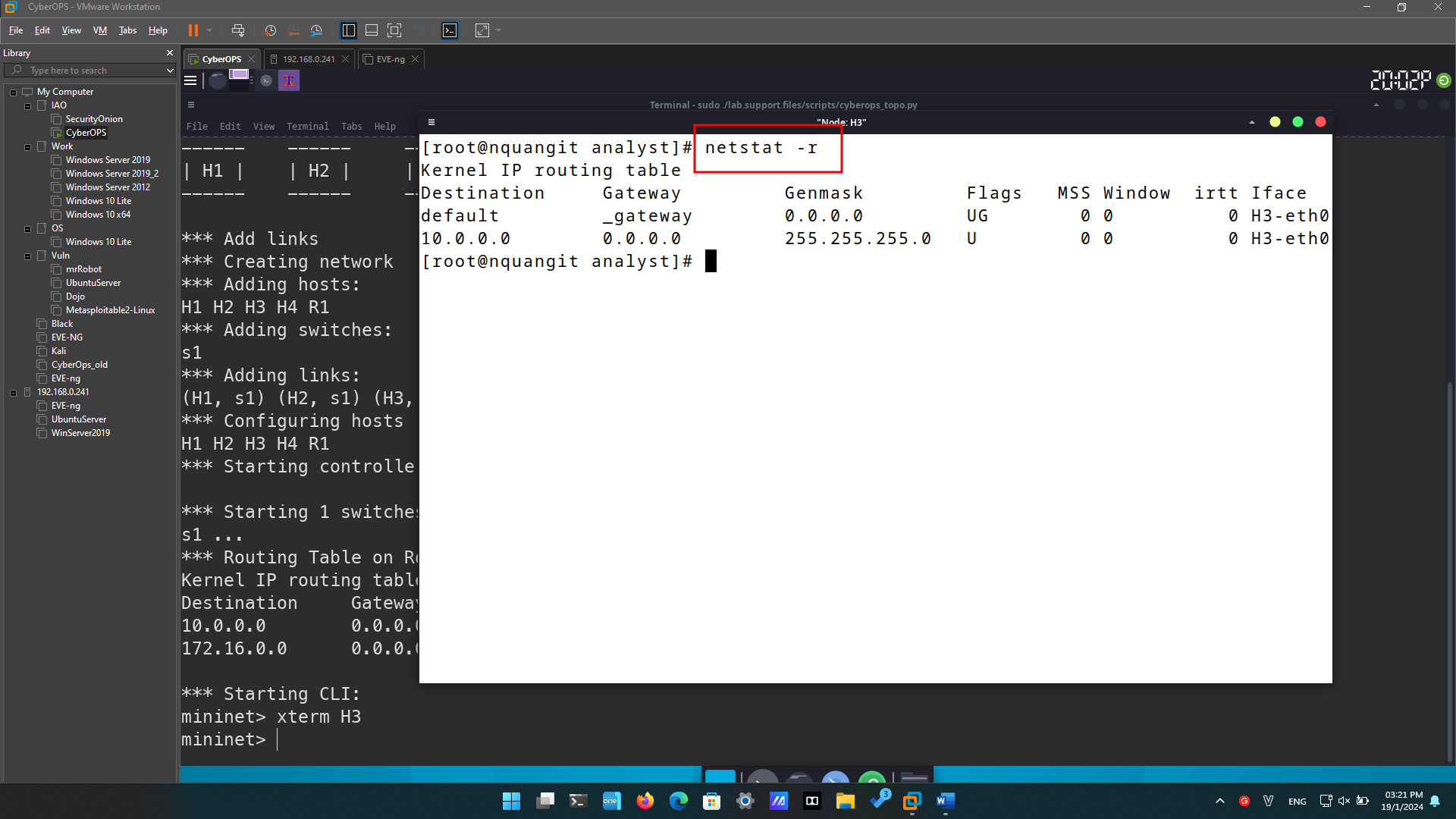
* + - 1. At the mininet prompt, start terminal windows on host H3.
      2. At the prompt on Node: h3, enter **ip address** to verify the IPv4 address and record the MAC address.

A screenshot of a computer

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Host-interface | IP Address | MAC Address |
| H3-eth0 | 10.0.0.13/24 | 6e:f6:a6:27:8c:26 |

* + - 1. At the prompt on Node: H3, enter **netstat -r** to display the default gateway information.



What is the IP address of the default gateway for the host H3?

0.0.0.0

\_gateway

### Clear the ARP cache on H3 and start capturing traffic on H3-eth0.

* + - 1. In the terminal window for Node: H3, enter **arp -n** to display the content of the ARP cache.

A screenshot of a computer

Description automatically generated

* + - 1. If there is any existing ARP information in the cache, clear it by enter the following command: **arp -d *IP-address***. Repeat until all the cached information has been cleared.

A screenshot of a computer

Description automatically generated

* + - 1. In the terminal window for Node: H3, open Wireshark and start a packet capture for H3-eth0 interface.

A screenshot of a computer

Description automatically generated

### Ping H1 from H3.

* + - 1. From the terminal on H3, ping the default gateway and stop after send 5 echo request packets.

A screenshot of a computer

Description automatically generated

* + - 1. After the ping is completed, stop the Wireshark capture.

### Filter Wireshark to display only ICMP traffic.

Apply the **icmp** filter to the captured traffic so only ICMP traffic is shown in the results.

A screenshot of a computer

Description automatically generated

### Examine the first Echo (ping) request in Wireshark.

* + - 1. In the Packet List pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. This should highlight the line blue.

A screenshot of a computer

Description automatically generated

* + - 1. Examine the first line in the Packet Details pane (middle section). This line displays the length of the frame; 98 bytes in this example.

A screenshot of a computer

Description automatically generated

* + - 1. The second line in the Packet Details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.

A screenshot of a computer

Description automatically generated

What is the MAC address of the PC’s NIC?

6e:f6:a6:27:8c:26

What is the default gateway’s MAC address?

66:f1:d3:4e:51:ce

* + - 1. You can click the arrow at the beginning of the second line to obtain more information about the Ethernet II frame.

A screenshot of a computer

Description automatically generated

What type of frame is displayed?

IPv4 (0x0800)

* + - 1. The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

A screenshot of a computer

Description automatically generated

What is the source IP address?

10.0.0.11

What is the destination IP address?

10.0.0.1

* + - 1. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the Packet Bytes pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the Packet Bytes pane.

A computer screen shot of a computer

Description automatically generated

* + - 1. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

A screenshot of a computer

Description automatically generated

1. What device and MAC address is displayed as the destination address?
2. Node H3’s MAC

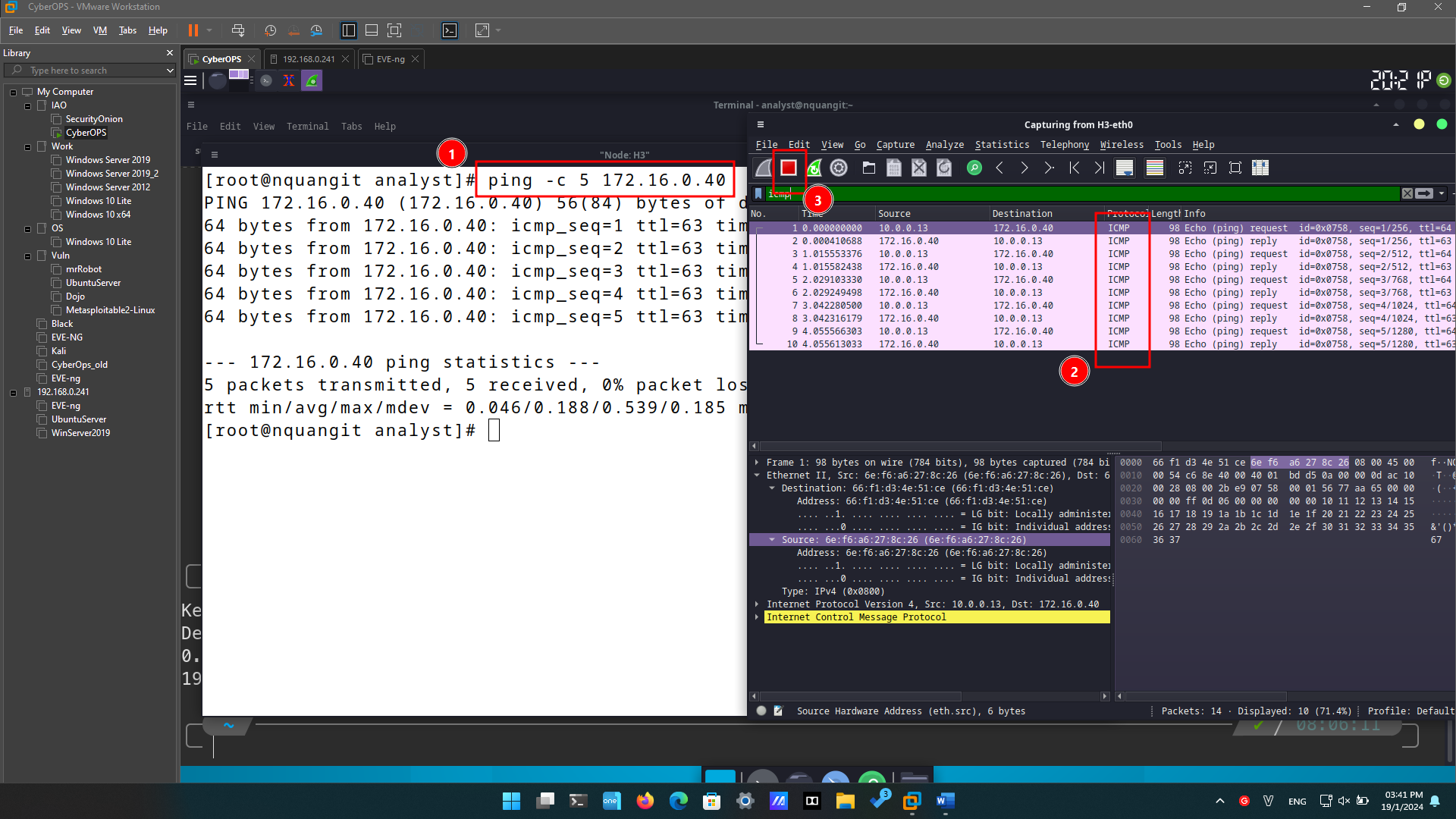
### Start a new capture in Wireshark.

* + - 1. Click the **Start Capture** icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click **Continue without Saving**.

A screenshot of a computer

Description automatically generated

* + - 1. In the terminal window of Node: H3, send 5 echo request packets to 172.16.0.40.
      2. Stop capturing packets when the pings are completed.



### Examine the new data in the packet list pane of Wireshark.

In the first echo (ping) request frame, what are the source and destination MAC addresses?

Source: 6e:f6:a6:27:8c:26

Dest: 66:f1:d3:4e:51:ce (Default Gateway)

What are the source and destination IP addresses contained in the data field of the frame?

Source: 10.0.0.13

Dest: 172.16.0.40

Compare these addresses to the addresses you received in Step 5. The only address that changed is the destination IP address.

Why has the destination IP address changed, while the destination MAC address remained the same?

When sending packets within a LAN, the MAC addresses of the source and destination devices are used. When packets go out to the Internet through a router, the MAC address of the router (default gateway) is typically used, while the IP addresses of the source and destination devices may change based on the external network.

# Reflection

1. Wireshark does not display the preamble field of a frame header. What does the preamble contain?

The preamble consists of seven octets featuring alternating 1010 sequences, along with an additional octet that serves as the frame's starting signal, marked by the sequence 10101011.