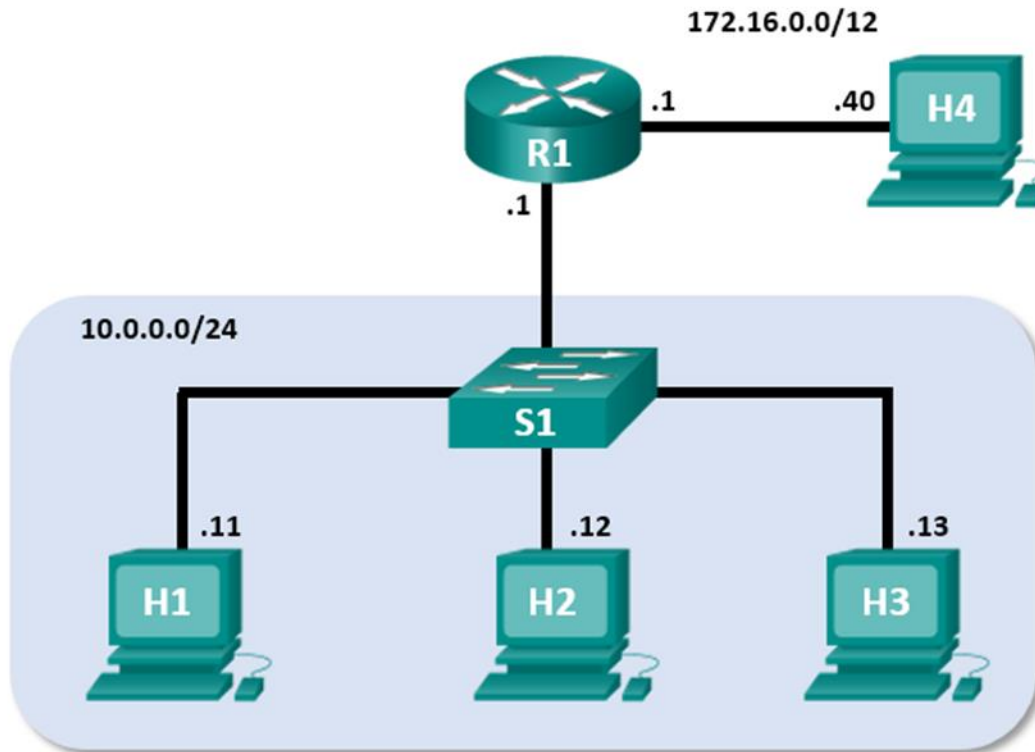


Lab - Using Wireshark to Examine Ethernet Frames



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	Broadcast (ff:ff:ff:ff:ff:ff)	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.						
Source Address	IntelCor_62:62:6d (f4:8c:50:62:62:6d)	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: <table><tr><th>Value</th><th>Description</th></tr><tr><td>0x0800</td><td>IPv4 Protocol</td></tr><tr><td>0x0806</td><td>Address resolution protocol (ARP)</td></tr></table>	Value	Description	0x0800	IPv4 Protocol	0x0806	Address resolution protocol (ARP)
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?

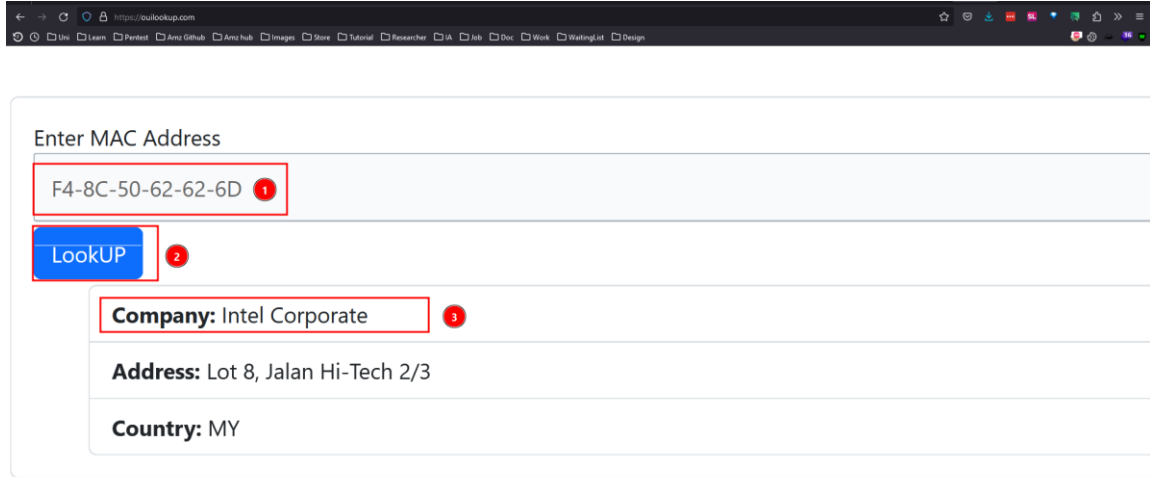
The PC can not send a ping request if it do not know the destination MAC address.

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



Enter MAC Address

F4-8C-50-62-62-6D 1

LookUP 2

Company:	Intel Corporate 3
Address:	Lot 8, Jalan Hi-Tech 2/3
Country:	MY

What portion of the MAC address is the OUI?

F4-8C-50

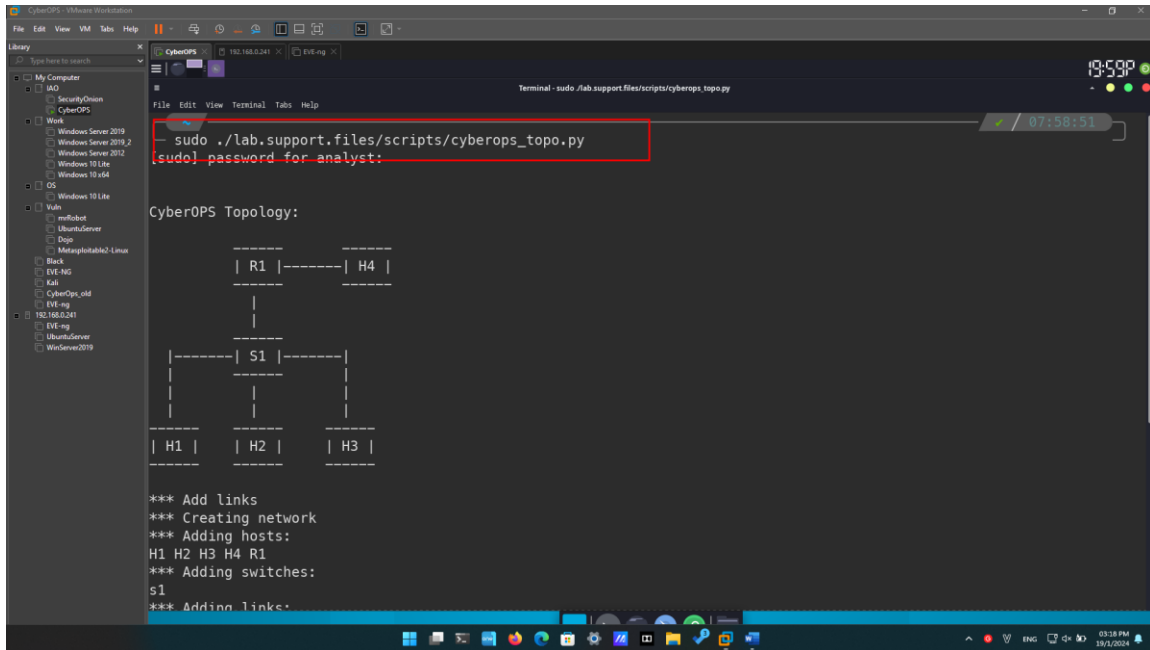
What is the Source's NIC serial number?

62-62-6D

Use Wireshark to Capture and Analyze Ethernet Frames

Examine the network configuration of H3.

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



```

sudo ./lab.support.files/scripts/cyberops_topo.py
[sudo] password for analyst:

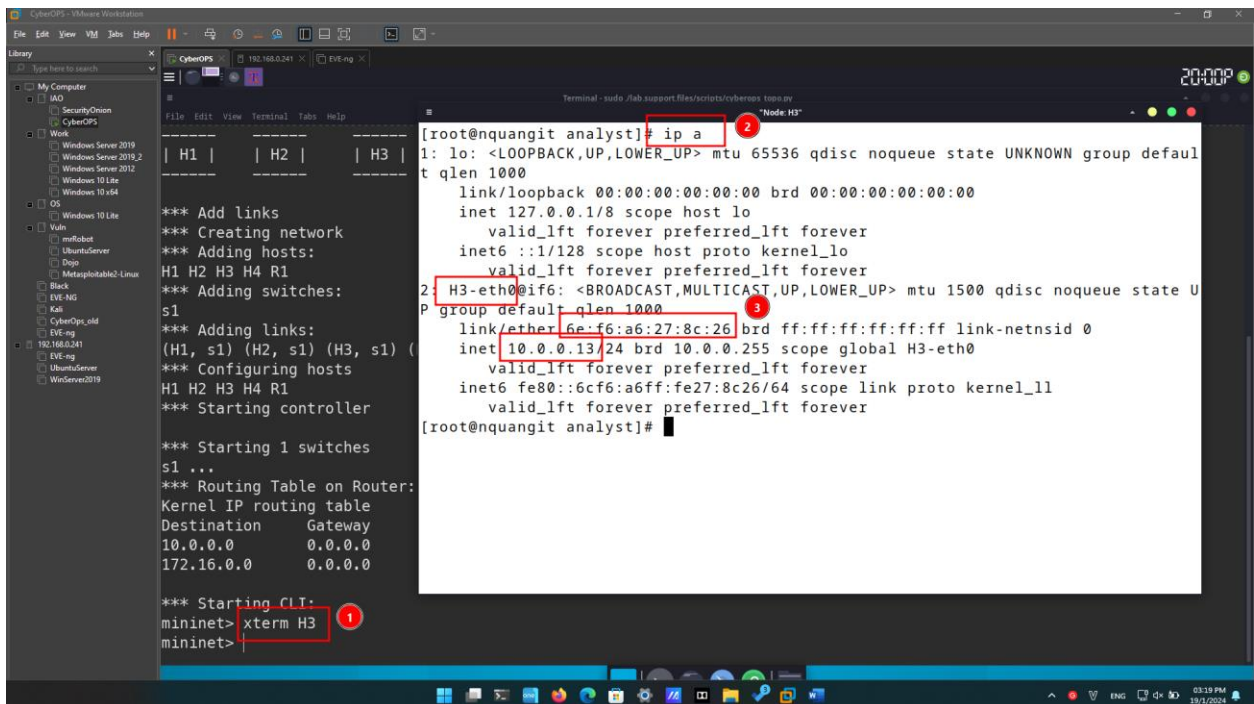
CyberOPS Topology:

  -----
  | R1 |-----| H4 |
  -----
  |
  -----
  |-----| S1 |-----|
  |
  -----
  | H1 |   | H2 |   | H3 |
  -----

*** Add links
*** Creating network
*** Adding hosts:
H1 H2 H3 H4 R1
*** Adding switches:
s1
*** Adding links:

```

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



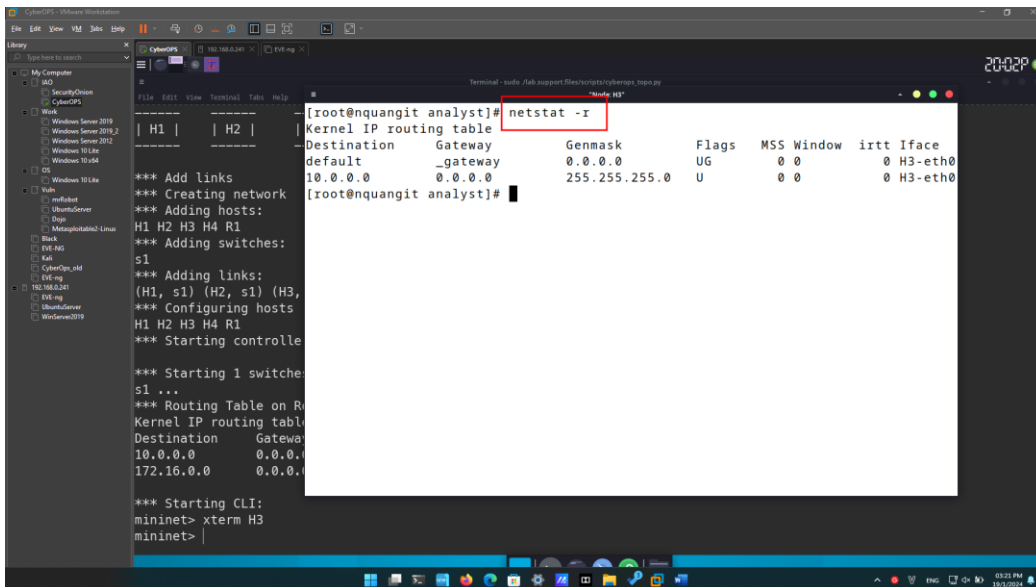
```

[roo@nquangit analyst]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
        valid_lft forever preferred_lft forever
2: H3-eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    group default qlen 1000
    link/ether 6e:f6:a6:27:8c:26 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.0.13/24 brd 10.0.0.255 scope global H3-eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::6cf6:a6ff:fe27:8c26/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
[roo@nquangit analyst]#

```

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

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



```

[Root@quangit analyst]# netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 _gateway 0.0.0.0 UG 0 0 0 H3-eth0
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 H3-eth0
[Root@quangit analyst]#
  
```

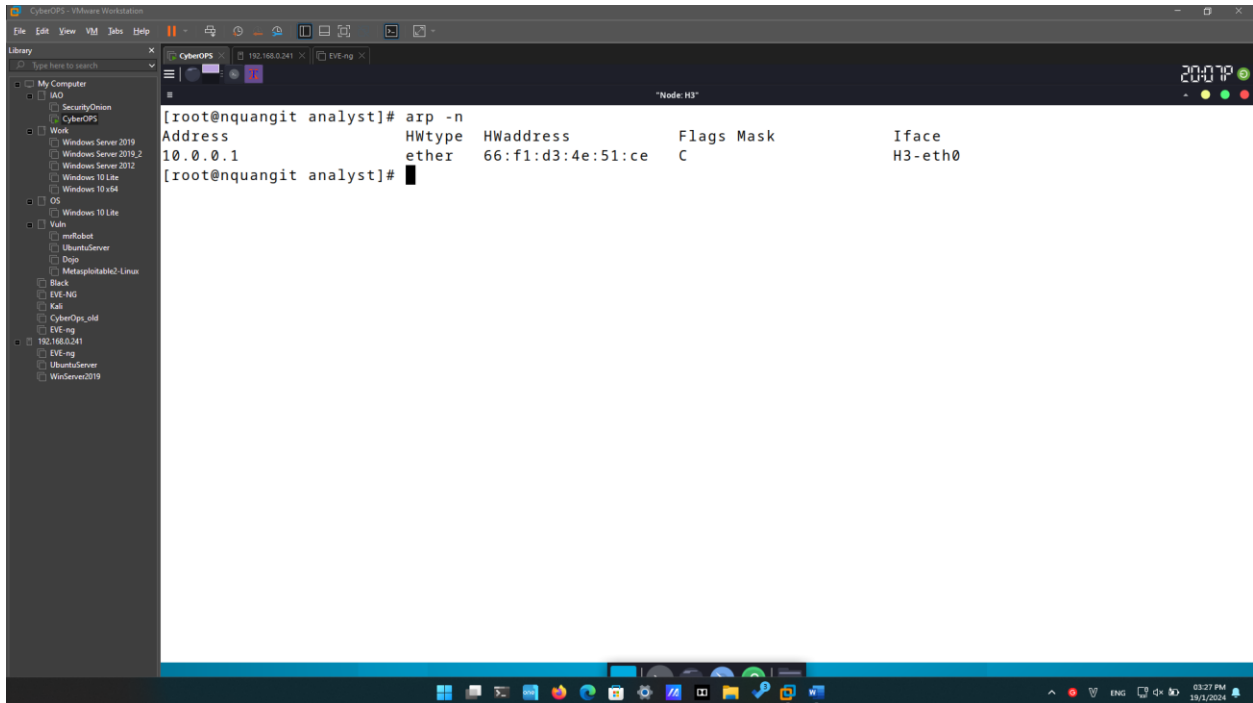
What is the IP address of the default gateway for the host H3?

0.0.0.0

_gateway

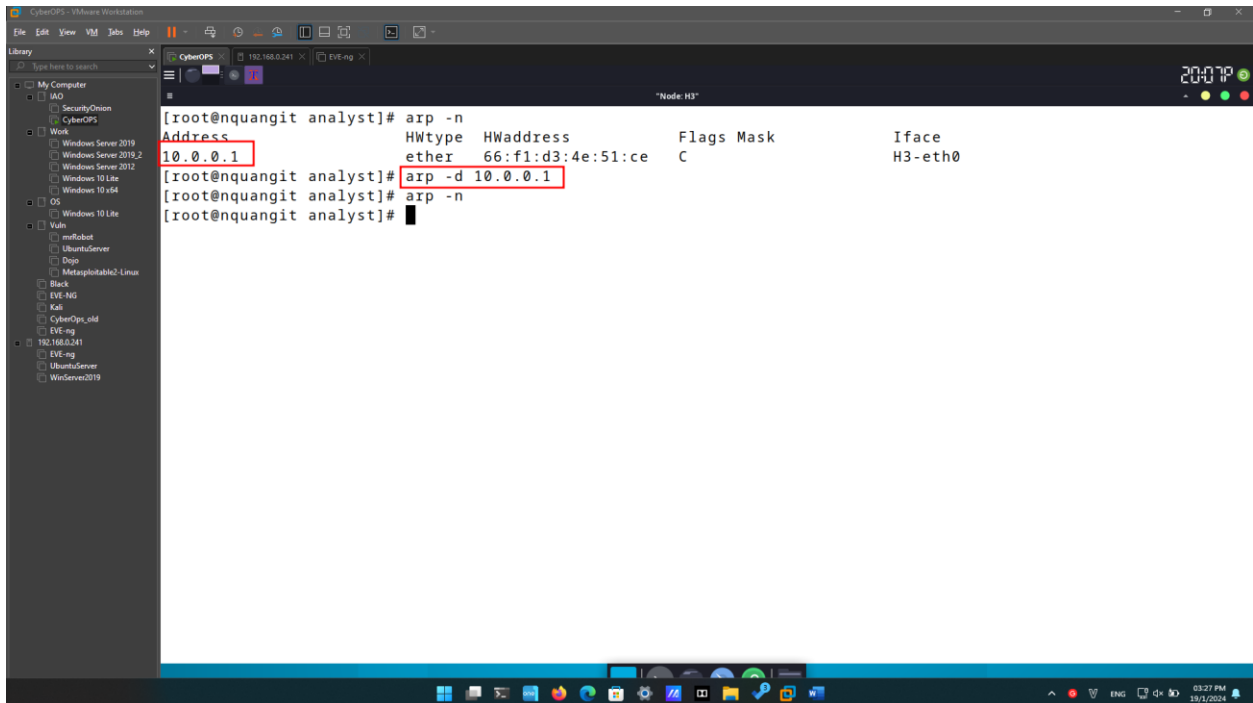
Clear the ARP cache on H3 and start capturing traffic on H3-eth0.

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



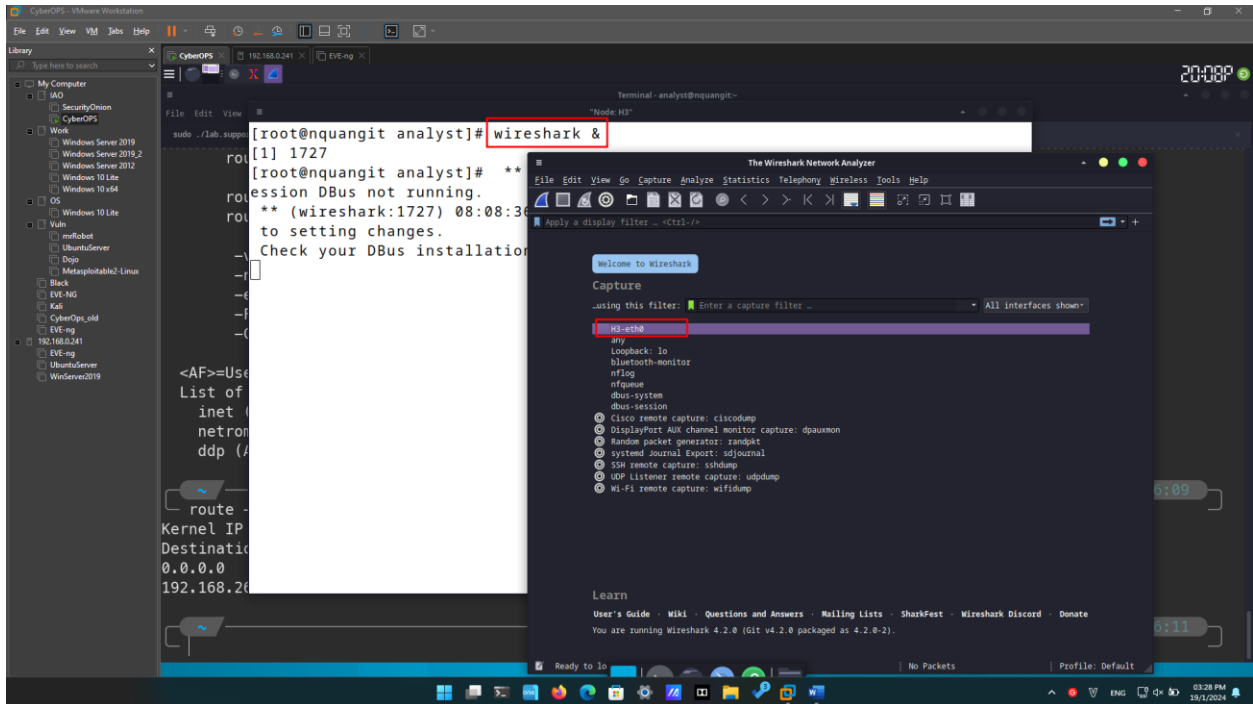
```
[root@quangit analyst]# arp -n
Address                  HWtype  HWaddress      Flags Mask            Iface
10.0.0.1                  ether    66:f1:d3:4e:51:ce    C                      H3-eth0
[root@quangit analyst]#
```

- b. 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.



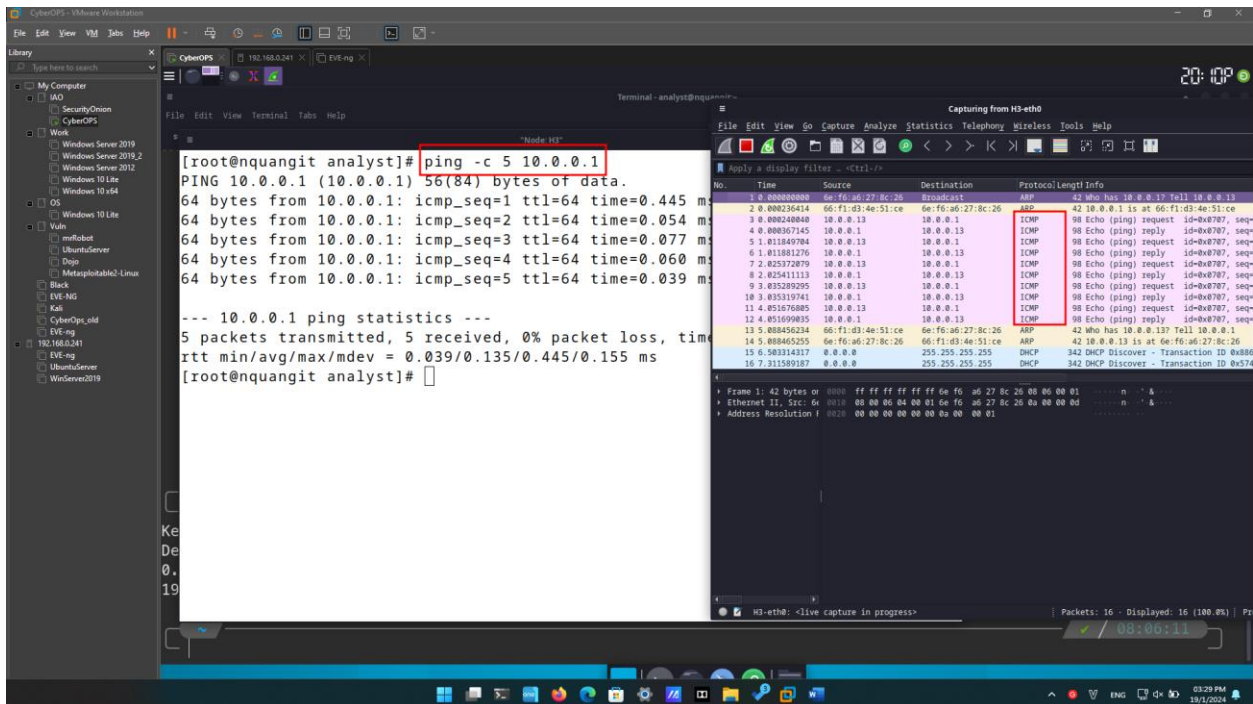
```
[root@quangit analyst]# arp -n
Address                  HWtype  HWaddress      Flags Mask            Iface
10.0.0.1                  ether    66:f1:d3:4e:51:ce    C                      H3-eth0
[root@quangit analyst]# arp -d 10.0.0.1
[root@quangit analyst]# arp -n
[root@quangit analyst]#
```

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



Ping H1 from H3.

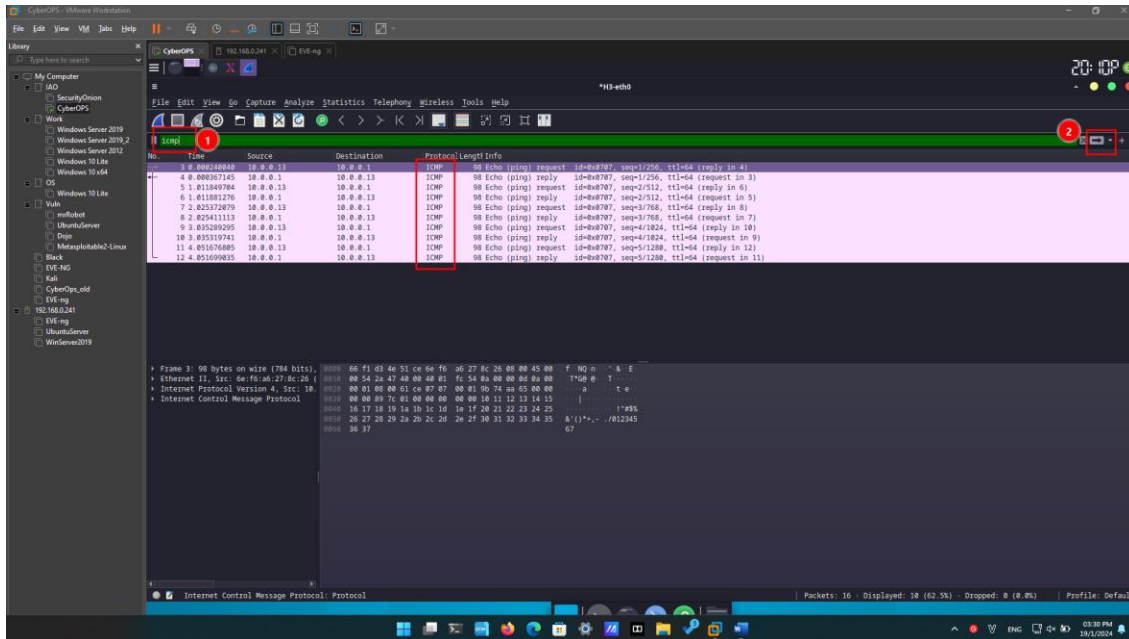
- From the terminal on H3, ping the default gateway and stop after send 5 echo request packets.



- After the ping is completed, stop the Wireshark capture.

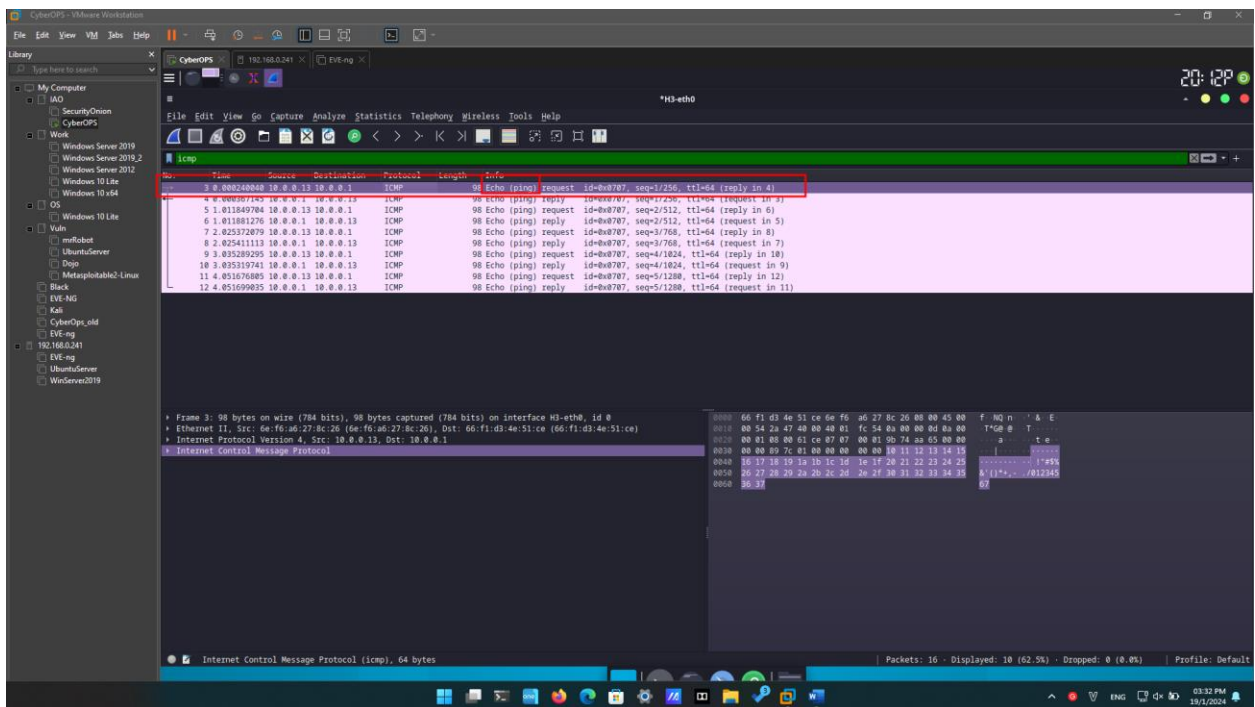
Filter Wireshark to display only ICMP traffic.

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

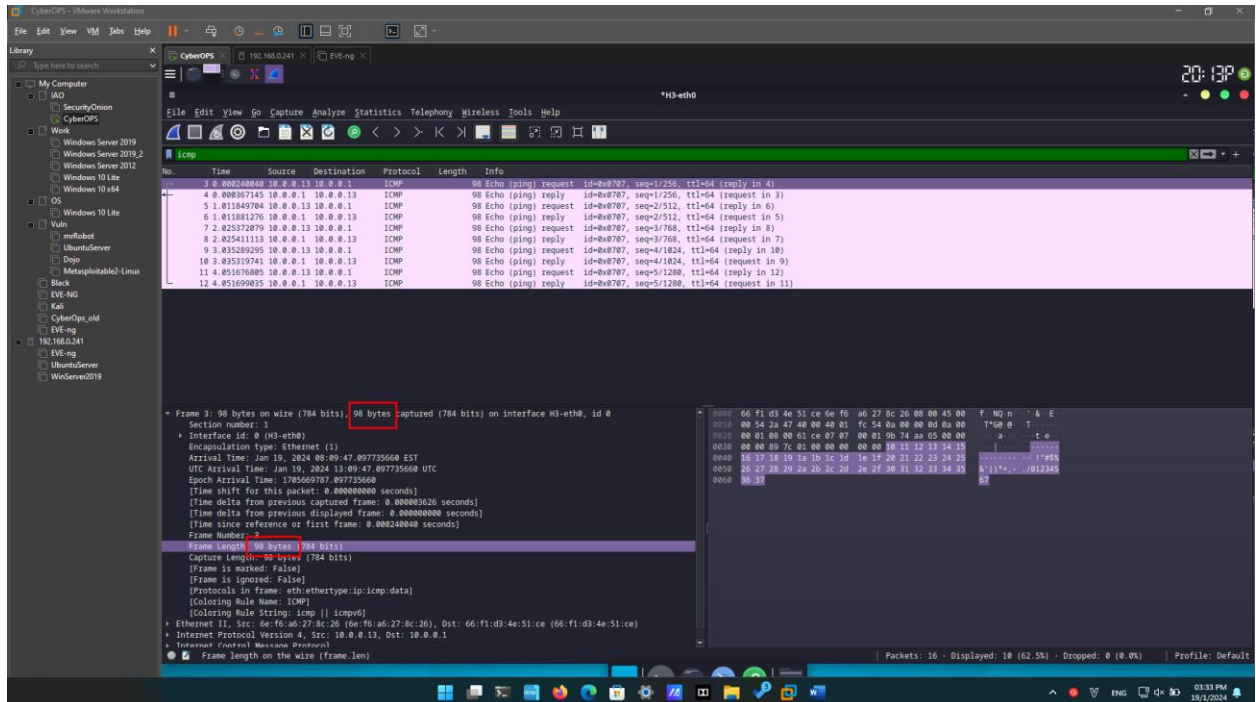


Examine the first Echo (ping) request in Wireshark.

- 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.

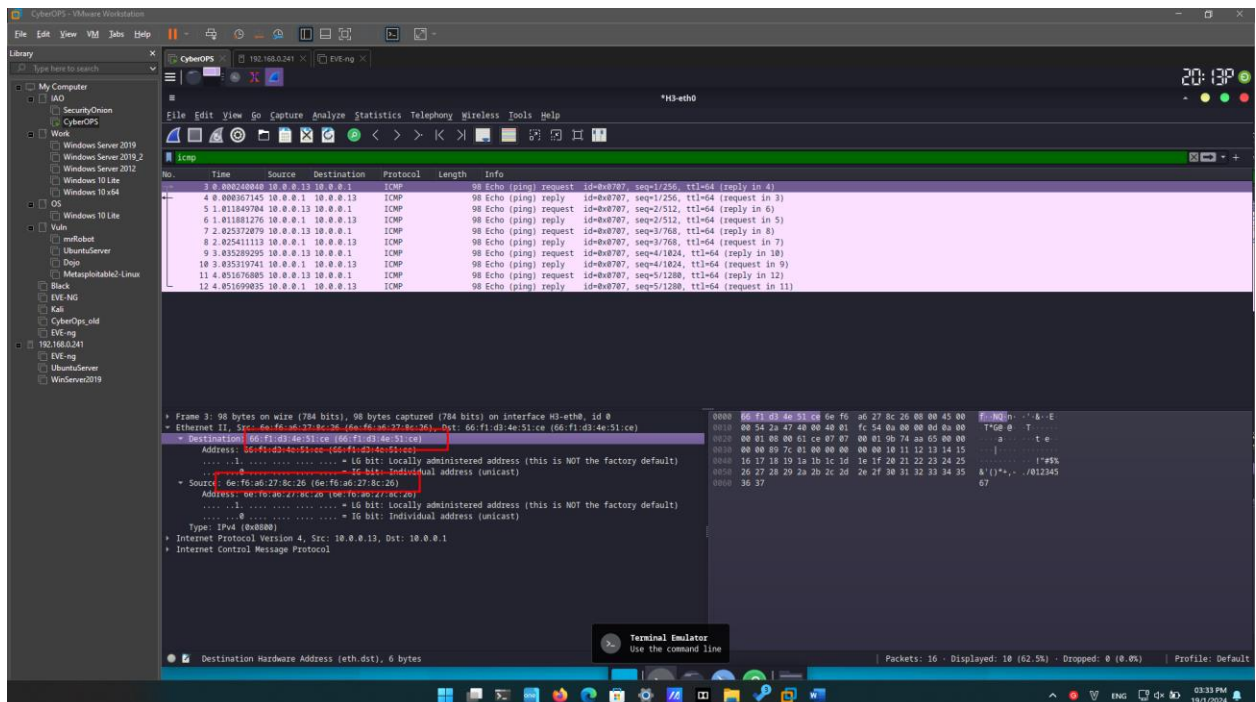


- b. Examine the first line in the Packet Details pane (middle section). This line displays the length of the frame; 98 bytes in this example.



The screenshot shows the Wireshark interface with the Packet Details pane expanded. The first line of the packet details is highlighted, showing the frame length: "Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface H3-eth0, id 0". The "98 bytes" is highlighted with a red box.

- c. 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.



The screenshot shows the Wireshark interface with the Packet Details pane expanded. The second line of the packet details is highlighted, showing the Ethernet II frame information: "Ethernet II, Src: 66:f1:d3:4e:51:ce (66:f1:d3:4e:51:ce), Dst: 66:f1:d3:4e:51:ce (66:f1:d3:4e:51:ce)". The source and destination MAC addresses are highlighted with red boxes.

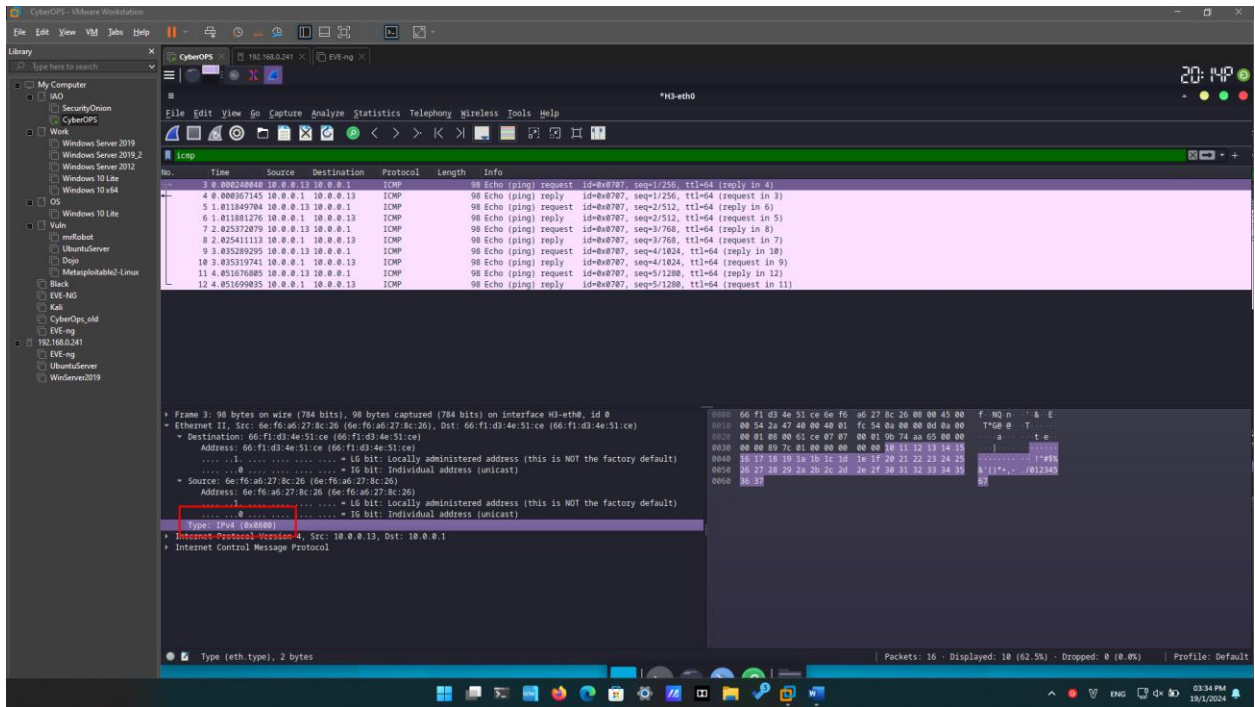
What is the MAC address of the PC's NIC?

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

What is the default gateway's MAC address?

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

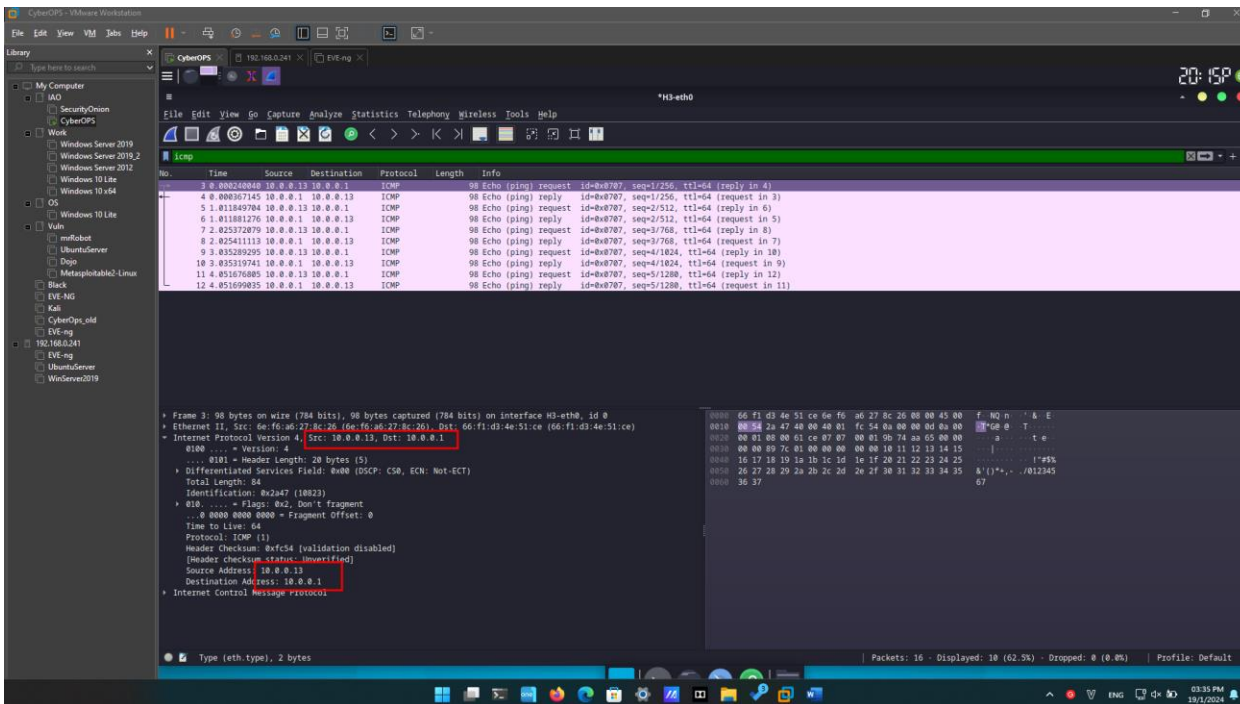
- d. You can click the arrow at the beginning of the second line to obtain more information about the Ethernet II frame.



What type of frame is displayed?

IPv4 (0x0800)

- e. 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.



The screenshot shows a Wireshark packet capture on the interface H3-eth0. The packet list displays several ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo request from 10.0.0.1 to 10.0.0.13. The packet details pane shows the source IP address as 10.0.0.13 and the destination IP address as 10.0.0.1.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000000	10.0.0.13	10.0.0.1	ICMP	98	Echo (ping) request id=0x0707, seq=17256, ttl=64 (reply in 4)
4	0.0000007145	10.0.0.1	10.0.0.13	ICMP	98	Echo (ping) reply id=0x0707, seq=17256, ttl=64 (request in 3)
5	1.011840704	10.0.0.13	10.0.0.1	ICMP	98	Echo (ping) request id=0x0707, seq=2/512, ttl=64 (reply in 6)
6	1.011841276	10.0.0.1	10.0.0.13	ICMP	98	Echo (ping) reply id=0x0707, seq=2/512, ttl=64 (request in 5)
7	2.025372879	10.0.0.13	10.0.0.1	ICMP	98	Echo (ping) request id=0x0707, seq=3/768, ttl=64 (reply in 8)
8	2.025411113	10.0.0.1	10.0.0.13	ICMP	98	Echo (ping) reply id=0x0707, seq=3/768, ttl=64 (request in 7)
9	3.032305295	10.0.0.13	10.0.0.1	ICMP	98	Echo (ping) request id=0x0707, seq=4/1024, ttl=64 (reply in 10)
10	3.032319741	10.0.0.1	10.0.0.13	ICMP	98	Echo (ping) reply id=0x0707, seq=4/1024, ttl=64 (request in 9)
11	4.051676885	10.0.0.13	10.0.0.1	ICMP	98	Echo (ping) request id=0x0707, seq=5/1280, ttl=64 (reply in 12)
12	4.051690835	10.0.0.1	10.0.0.13	ICMP	98	Echo (ping) reply id=0x0707, seq=5/1280, ttl=64 (request in 11)

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface H3-eth0, id 0
 Ethernet II, Src: 66:f6:a6:27:8c:26, Dst: 66:f1:d3:4e:51:ce (66:f1:d3:4e:51:ce)
 Internet Protocol Version 4, Src: 10.0.0.13, Dst: 10.0.0.1
 ICMP Echo (ping) request id=0x0707, seq=17256, ttl=64 (reply in 4)
 Total Length: 84
 Identification: 0x2a47 (10023)
 Flags: 0x2, Don't fragment
 Time to Live: 64
 Protocol: ICMP (1)
 Header Checksum: 0x7c54 (validation disabled)
 Source Address: 10.0.0.13
 Destination Address: 10.0.0.1
 Internet Control Message Protocol

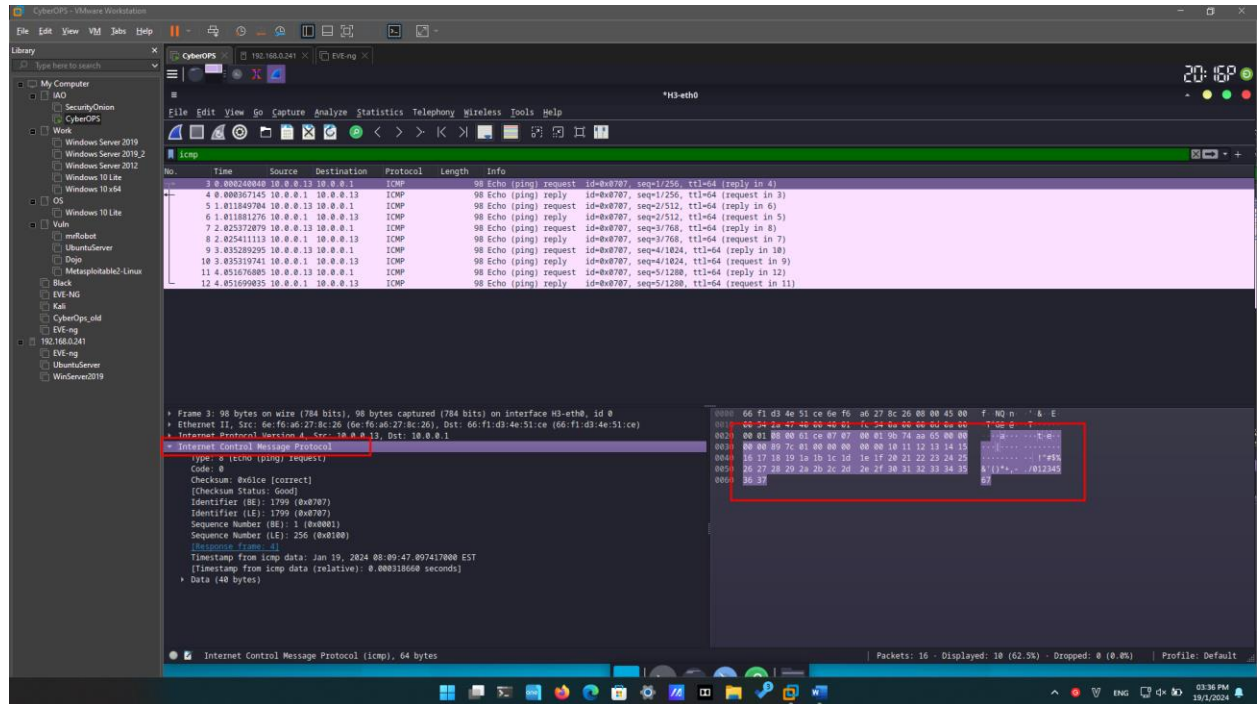
What is the source IP address?

10.0.0.13

What is the destination IP address?

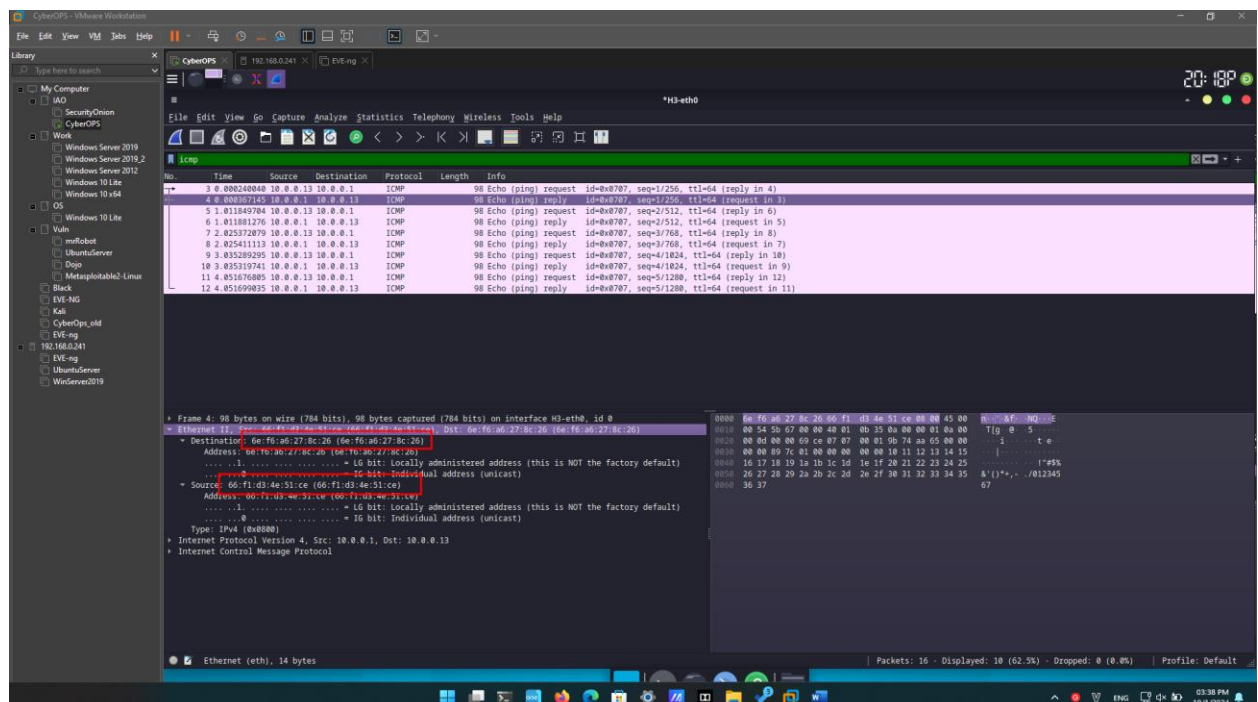
10.0.0.1

- f. 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.



The screenshot shows the Wireshark interface with a packet capture on the 'H3-eth0' interface. The packet list shows a series of ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo (ping) request with sequence number 1256. The packet details pane shows the ICMP Echo (ping) request with a sequence number of 1256. The packet bytes pane shows the raw data of the ICMP Echo request, with the 'f' flag highlighted in red.

- g. 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.



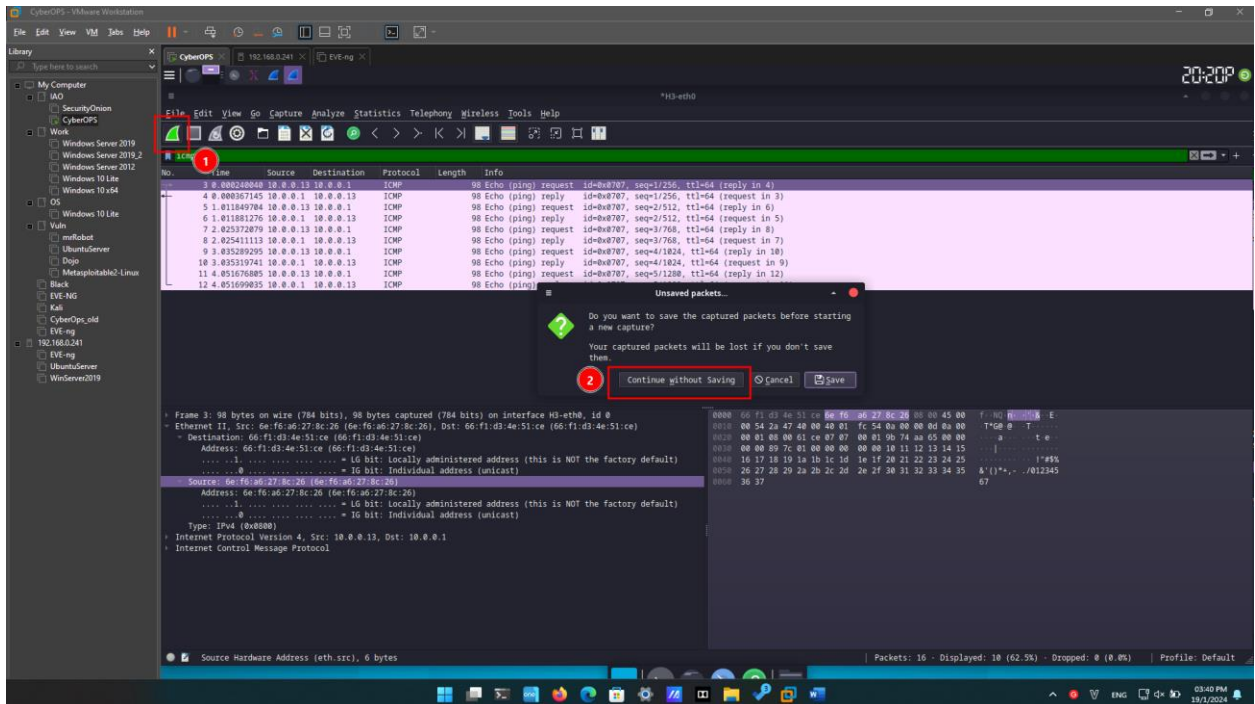
The screenshot shows the Wireshark interface with a packet capture on the 'H3-eth0' interface. The packet list shows a series of ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo (ping) reply with sequence number 1256. The packet details pane shows the ICMP Echo (ping) reply with a sequence number of 1256. The packet bytes pane shows the raw data of the ICMP Echo reply, with the 'f' flag highlighted in red.

What device and MAC address is displayed as the destination address?

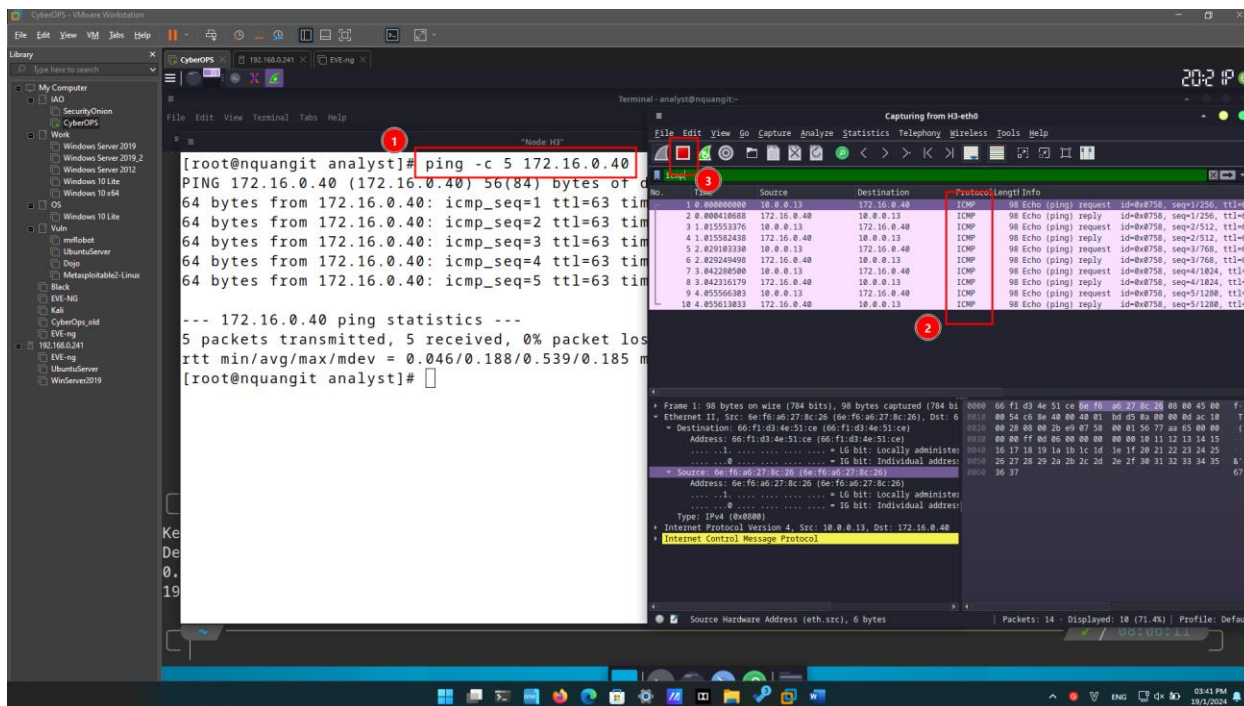
Node H3's MAC

Start a new capture in Wireshark.

- 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**.



- In the terminal window of Node: H3, send 5 echo request packets to 172.16.0.40.
- 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

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.