**TUGAS TEORI**

**MINGGU 5**

**KONSEP JARINGAN**

****

Disusun oleh:

**Muhammad Zaid Abdillah**

**2110191013**

**PROGRAM STUDI D-IV TEKNIK INFORMATIKA**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

Lab - Use Wireshark to Examine Ethernet Frames Topology

**Objectives**

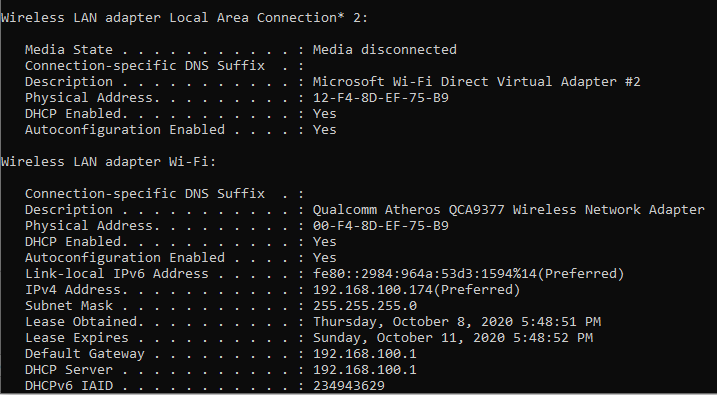
Part 1 - Examine the Header Fields in an Ethernet II Frame

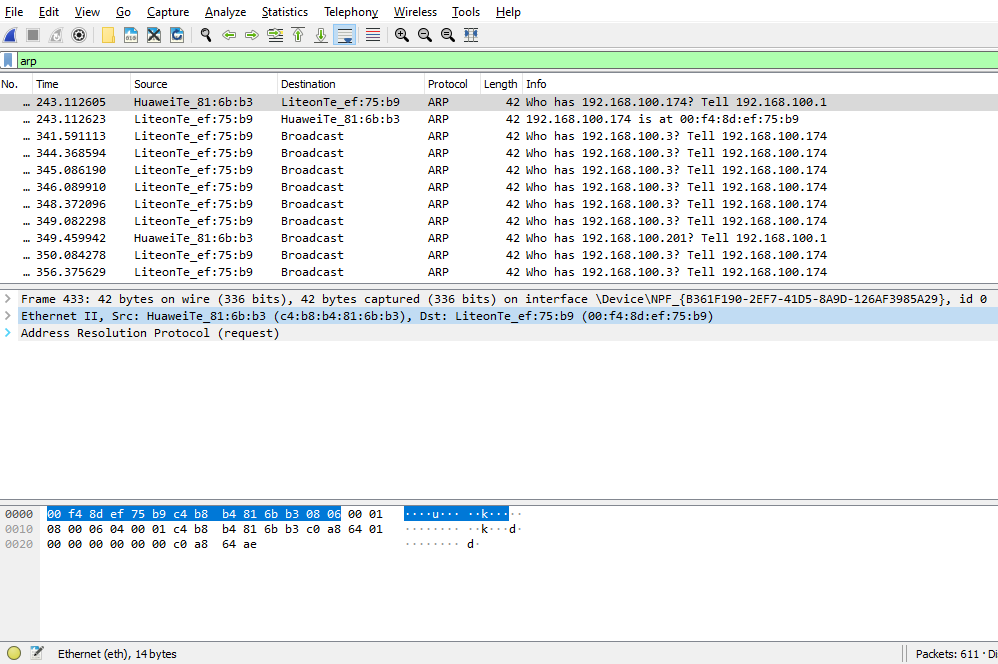
Step 1 - Review the Ethernet II header field descriptions and lengths.

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

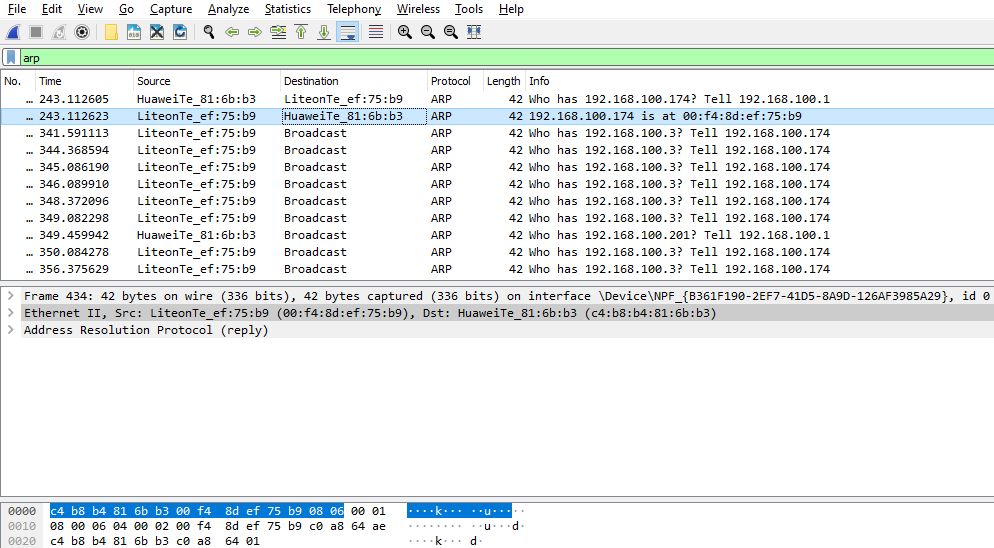
Step 2 - Examine the network configurations of the PC

Jawab : Laptop saya drivernya en0 dengan IP "​192.168.​100.174" dengan MAC address "12:f4:8d:ef:75:b9".



Step 3 - Examine Ethernet frames in a Wireshark captureJawab :ARP Request 

ARP Reply



Step 4 - Step 4: Examine the Ethernet II header contents of an ARP request

Jawab :

|  |  |  |  |
| --- | --- | --- | --- |
| Fields | Value |  | Descriptions |
|  |  |  |  |
| Preamble | Tidak ada pada screenshot |  | Bagian ini berisi sinkronisasi bit, diproses |
|  |  |  | oleh perangkat NIC. |
|  |  |  |  |
| Destination Address |  |  |  |
|  |  |  |  |
| Source Address |  |  |  |
|  |  |  |  |
| Frame Type |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Fields | Value |  | Descriptions |
|  |  |  | |
| Preamble | Tidak ada pada | Bagian ini berisi sinkronisasi bit, diproses oleh | |
|  | screenshot | perangkat NIC. | |
|  |  |  | |
| Destination Address | Broadcast | Layer 2 untuk tiap frame. Setiap alamat memiliki | |
|  | (c4:b8:b4:81:6b:b3) | panjang 48 bit, atau 6 oktet, dinyatakan sebagai | |
|  |  | 12 digit heksadesimal, 0-9, A-F. Format umum | |
|  |  | adalah 12: 34: 56: 78: 9A: BC. | |
| Source Address |  | Enam nomor hex pertama menunjukkan | |
|  | LiteonTe\_ef:75:b9 | manufaktur dari network interface card (NIC), | |
|  | (00:f4:8d:ef:75:b9) | enam nomor hex terakhir adalah nomor seri NIC. | |
|  |  |  | |
| Frame Type | 0x0806 | Untuk frame Ethernet II, kolom ini berisi nilai | |
|  |  | heksadesimal yang digunakan untuk | |
|  |  | menunjukkan jenis protokol lapisan atas di kolom | |
|  |  | data. Ada banyak protokol lapisan atas yang | |
|  |  | didukung oleh Ethernet II. Dua jenis bingkai | |
|  |  | yang umum adalah ini: | |
|  |  | Deskripsi Nilai | |
|  |  | 0x0800​ Protokol IPv4 | |
|  |  | 0x0806​ Address Resolution Protocol (ARP) | |
| Data | ARP | Berisi protokol tingkat atas yang dienkapsulasi. | |
|  |  | Bidang data antara 46 - 1.500 byte. | |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| FCS | Tidak ada pada | Frame Check Sequence, digunakan oleh NIC |
|  | screenshot | untuk mengidentifikasi kesalahan selama |
|  |  | transmisi. Nilai dihitung oleh perangkat |
|  |  | pengirim, meliputi alamat bingkai, jenis, dan |
|  |  | bidang data. Ini diverifikasi oleh penerima. |
|  |  |  |

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

Jawab :

Semua host di LAN akan menerima frame broadcast ini. Host dengan alamat IP 192.168.100.1 (gateway default) akan mengirimkan balasan unicast ke sumber (host PC). Balasan ini berisi alamat MAC dari NIC gateway default.

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

Jawab :

Sebelum PC dapat mengirim permintaan ping ke host, PC perlu menentukan alamat MAC tujuan sebelum dapat membuat header frame untuk ping request tersebut. Broadcast ARP digunakan untuk meminta alamat MAC dari host dengan alamat IP yang terdapat dalam ARP.

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

Jawab :

MAC address sourcenya adalah "00:f4:8d:ef:75​:b9".

What is the Vendor ID (OUI) of the Source NIC in the ARP reply?

Jawab :

Vendor nya adalah "​HuaweiTe​".

What portion of the MAC address is the OUI?

Jawab :

3 oktet pertama dari alamat MAC menunjukkan OUI.

What is the NIC serial number of the source?

jawab :

NIC serial nya adalah "​81:6b:​b3".

Part 2 - Use Wireshark to Capture and Analyze Ethernet Frames

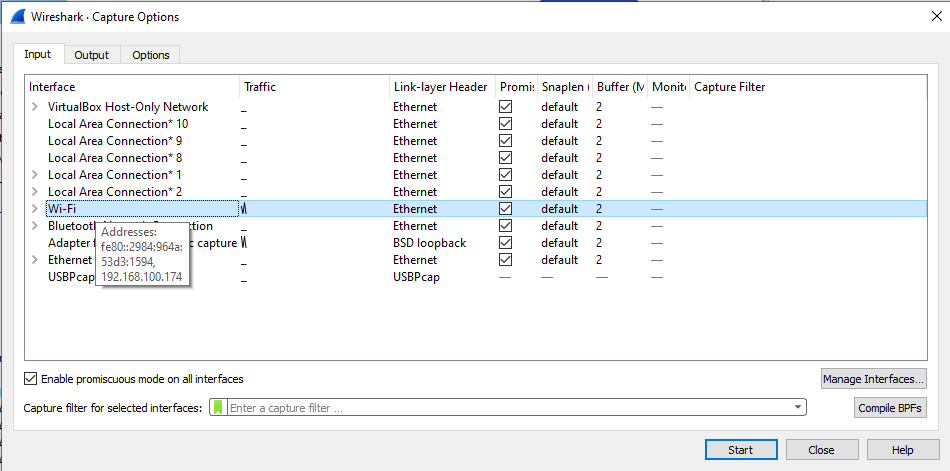
Step 1 - Determine the IP address of the default gateway on your PC. Open a command prompt window and issue the ​**ipconfig**​command. What is the IP address of the PC default gateway?

Jawab :

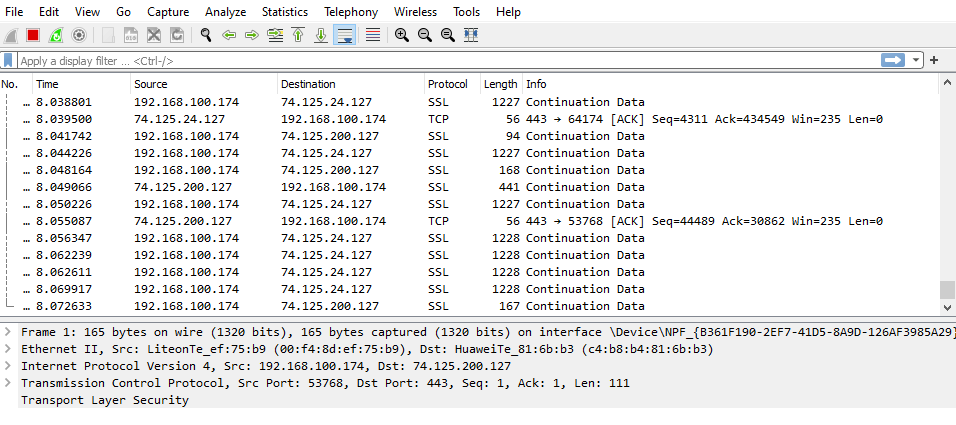
IP address "192.168.1.102" dan Gateway "192.168.100.1".

Step 2 - Step 2: Start capturing traffic on your PC NIC.

a. Open wireshark to start data capture.



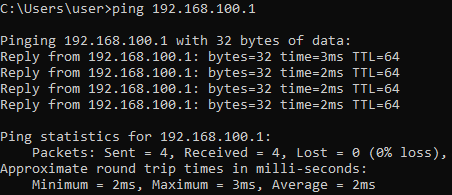
b. Observe the traffic that appears in the packet list window.



Step 3 - Filter Wireshark to display only ICMP traffic



Step 4 - From the command prompt window, ping the default gateway of your PC.

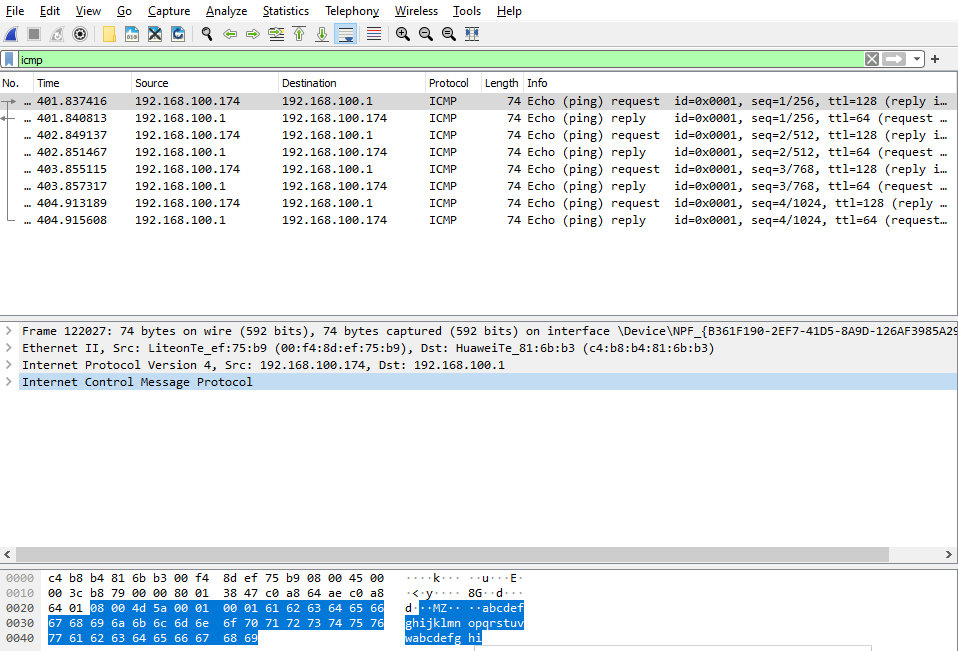


Step 5 - Stop capturing traffic on the NIC.



Step 6 - Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the packet list pane (top), the Packet Details pane (middle), and the Packet Bytes pane (bottom). If you selected the correct interface for packet capturing previously, Wireshark should display the ICMP information in the packet list pane of Wireshark.



1. In the packet list pane (top section), click the first frame listed. You should see ​**Echo (ping)** **request**​under the​**Info**​heading. The line should now be highlighted.
2. Examine the first line in the packet details pane (middle section). This line displays the length of the frame.

Jawab :

Panjang frame nya 98 Bytes.

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.

What is the MAC address of the PC NIC? Jawab :

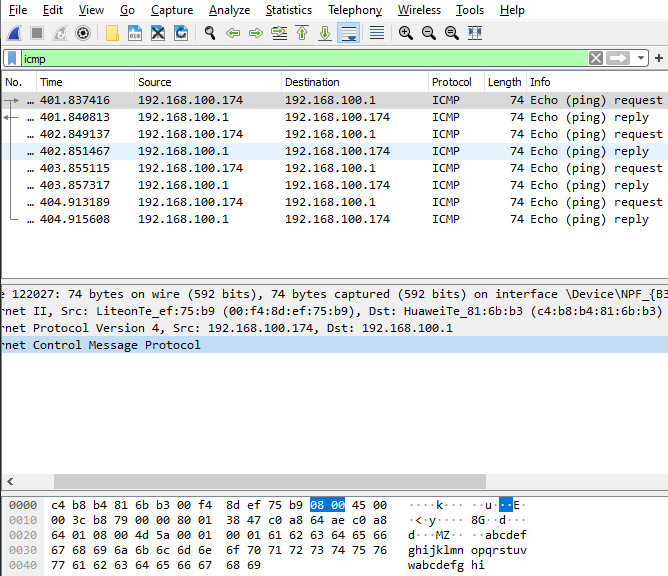
MAC address " 00-F4-8D-EF-75-B9".

What is the default gateway’s MAC address?

Jawab :

Default gateway MAC address "c4:b8:b4:81:6b:b3".

1. You can click the greater than (>) sign at the beginning of the second line to obtain more information about the Ethernet II frame.



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. What is the source IP address?

Jawab :

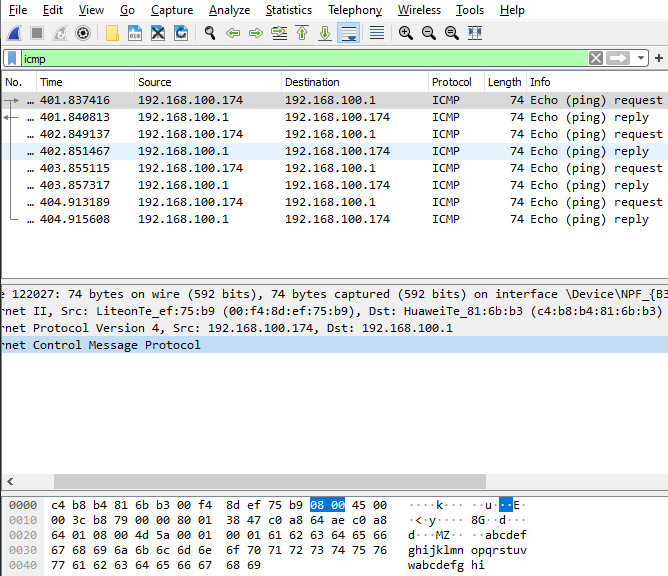
Source IP address " 192.168.100.174​".

What is the destination IP address? Jawab :

Destination IP address "​192.168.100.1​".

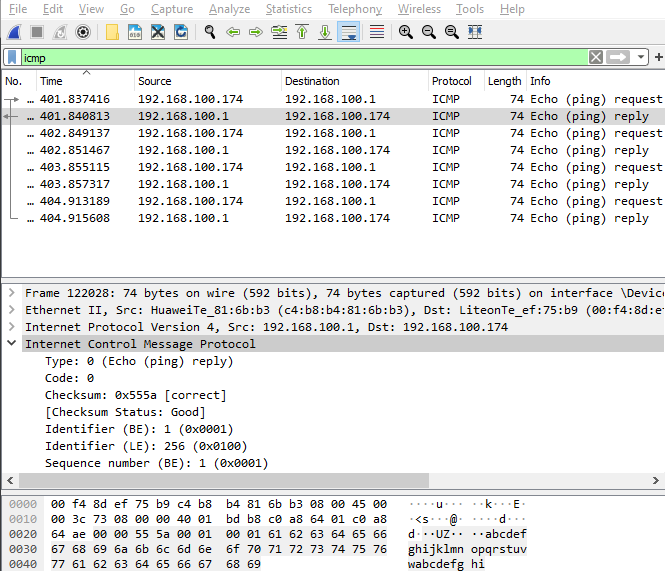
1. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the ​**Packet Bytes**​pane (bottom section). Click the ​**Internet Control Message** **Protocol**​line in the middle section and examine what is highlighted in the​**Packet Bytes** pane.

What do the last two highlighted octets spells? Jawab :



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.

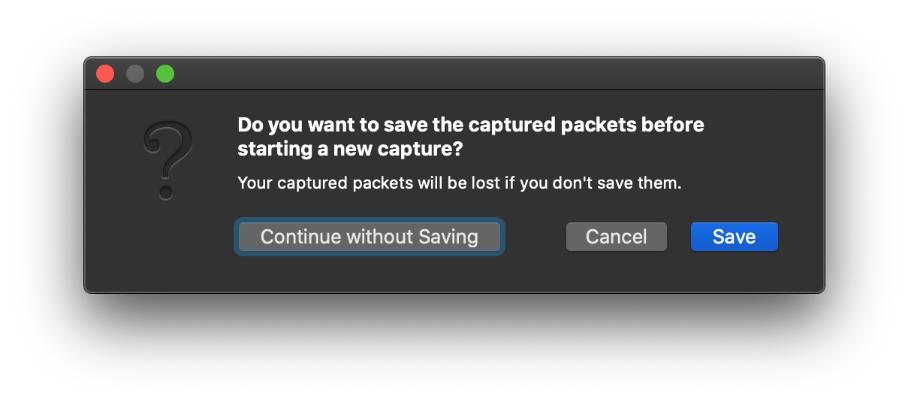
What device and MAC address is displayed as the destination address? Jawab :



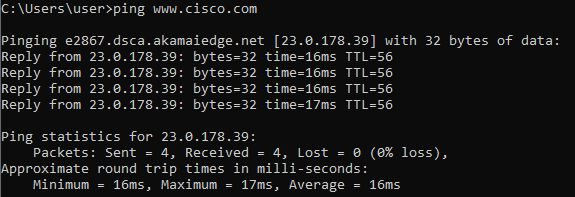
Laptop saya, MAC address "00-F4-8D-EF-75-B9".

Step 7 - Capture packets for a remote host.

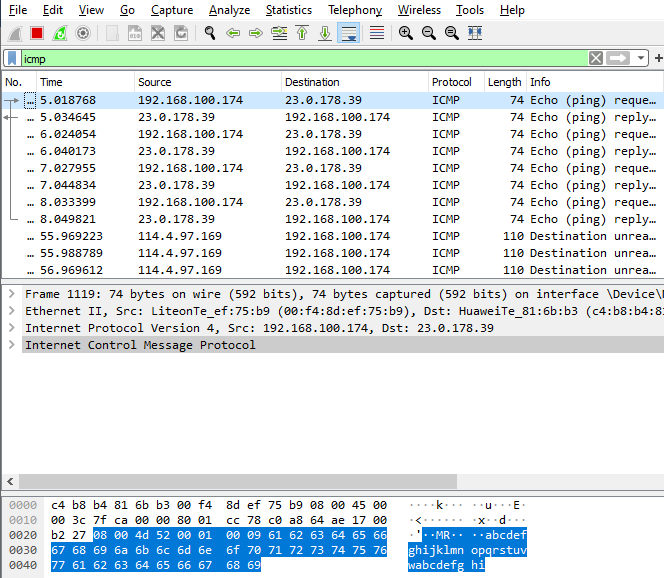
1. Click the ​**Start Capture**​icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click ​**Continue without Saving**​.



b. In a command prompt window, ping ​[www.cisco.com](http://www.cisco.com/)​.



c. Stop capturing packets.



1. 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? Jawab :

Source MAC address "00:f4:8d:ef:75b9". Destination MAC address "c4:b8:b4:81:6b:b3".

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

Source IP address "192.168.100.174". Destination IP address " 192.168.100.1".

Compare these addresses to the addresses you received in Step 6. 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?

Jawab :

Karena pada step 7 ini yang kita ping adalah ​[*www.cisco.com*](http://www.cisco.com/)*​*.Sedangkan pada step 6 kita melakukan ping terhadap gateway kita sendiri.