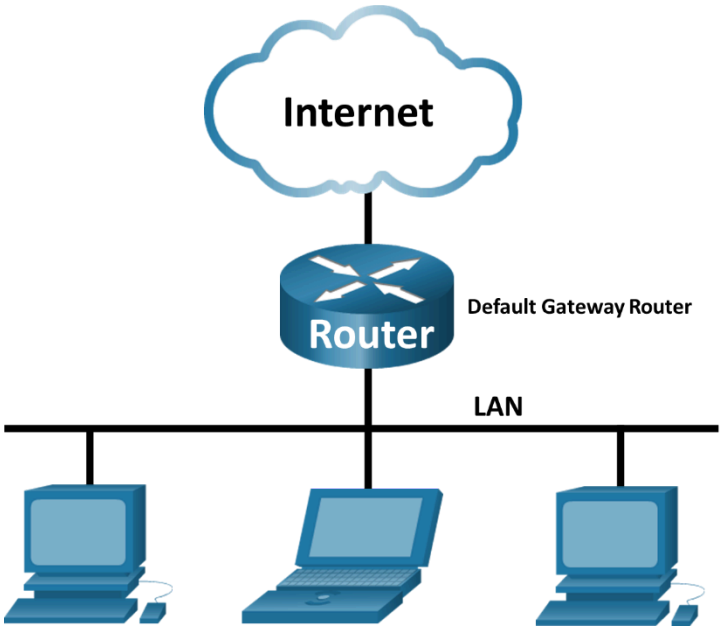
Lab - View Captured Traffic in Wireshark

Topology



Objectives

Part 1: Download and Install Wireshark

Part 2: Capture and Analyze ARP Data in Wireshark

- Start and stop data capture of ping traffic to remote hosts.
- Locate the IPv4 and MAC address information in captured PDUs.
- Analyze the content of the ARP messages exchanged between devices on the LAN.

Part 3: View the ARP cache entries on the PC

- Access the Windows Command Prompt.
- Use the Windows arp command to view the local ARP table cache on the PC.

Background / Scenario

Address Resolution Protocol (ARP) is used by TCP/IP to map a Layer 3 IPv4 address to a Layer 2 MAC address. When an Ethernet frame is transmitted on the network, it must have a destination MAC address. To dynamically discover the MAC address of a known destination, the source device broadcasts an ARP request on the local network. The device that is configured with the destination IPv4 address responds to the request with an ARP reply and the MAC address is recorded in the ARP cache.

Every device on the LAN maintains its own ARP cache. The ARP cache is a small area in RAM that holds the ARP responses. Viewing an ARP cache on a PC displays the IPv4 address and the MAC address of each device on the LAN with which the PC has exchanged ARP messages.

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate protocol specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the Cisco courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark, although it may already be installed. In this lab, you will use Wireshark to capture ARP exchanges on the local network.

Required Resources

- 1 PC (Windows 10)
- internet access
- Additional PC(s) on a local-area network (LAN) will be used to reply to **ping** requests. If no additional PCs are on the LAN, the default gateway address will be used to reply to the **ping** requests.

Instructions

Part 1: Download and Install Wireshark

Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux.

If Wireshark is already installed on your PC, you can skip Part 1 and go directly to Part 2. If Wireshark is not installed on your PC, check with your instructor about your academy's software download policy.

Step 1: Download Wireshark.

a. Wireshark can be downloaded from www.wireshark.org.

b. Click **Download**.

c. Choose the software version you need based on your PC's architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.

d. After making the selection, the download should start. Click **Save File** if prompted. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

Step 2: Install Wireshark.

a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process.

b. Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you maybe prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.

c. If this is the first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.

d. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.

e. Keep the default settings on the Choose Components window and click **Next**.

f. Choose your desired shortcut options and click **Next**.

g. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.

h. To capture live network data, Npcap must be installed on your PC. If your installed version of Npcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install Npcap x.x.x** (version number) check box. Click **Next**.

i. A separate window opens up for Npcap Setup. Click **I Agree** to in the Npcap License Agreement window. In the Installation Options window, leave all the checkboxes unselected and click **Install** to install Npcap. Click **Next** when finished. Click **Finish** to close the wizard.

j. The installation of USBPcap is not necessary for this course. It is only required if you are planning to capture USB traffic. Click **Install** to start the installation.

Note: **Because USBPcap is experimental, make sure that you have created a system restore point before the installation of USBPcap.**

k. Wireshark starts installing its files and a separate window displays with the status of the installation. Click **Next** when the installation is complete.

l. Click **Finish** to complete the Wireshark install process. If the installation process is stalled, verify that the Npcap installation is finished. Click **Next** to continue.

m. Reboot the PC to finish the installation.

Part 2: Capture and Analyze Local ARP Data in Wireshark

In Part 2 of this lab, you will ping another PC on the LAN and capture ARP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IPv4 address and the MAC address.

a. Navigate to a Command Prompt window, type **ipconfig /all** at the prompt.

b. Note which network adapter that the PC is using to access the network. Record your PC interface's IPv4 address and MAC address (Physical Address).

```
C:\Users\Student> ipconfig /all
<output omitted>
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : A4-AE-31-AD-78-4C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f9e7:e41d:a772:f993%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, August 04, 2016 05:35:35 PM
   Lease Expires . . . . . . . . . . : Friday, August 05, 2016 05:35:35 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 245648945
```

```
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-87-BF-52-A4-4E-31-AD-78-4C
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

c. Ask a team member for their PC's IPv4 address and give your PC's IPv4 address to them. Do not provide them with your MAC address at this time.

   Record the IPv4 addresses of the default gateway and the other PCs on the LAN.

Step 2: Start Wireshark and begin capturing data.

a. On your PC, click **Start** and type **Wireshark**. Click **Wireshark Desktop App** when it appears in the search results window.

Note: Alternatively, your installation of Wireshark may also provide a Wireshark Legacy option. This displays Wireshark in the older but widely recognized GUI. The remainder of this lab was completed using the newer Desktop App GUI.

b. After Wireshark starts, select the network interface that you identified with the **ipconfig** command. Enter **arp** in the filter box. This selection configures Wireshark to only display packets that are part of the ARP exchanges between the devices on the local network. After you have selected the correct interface and entered the filter information, click **Start capturing packets** (shark fin icon) to begin the data capture.

   Information will start scrolling down the top section in Wireshark. Each line represents a message being sent between a source and destination device on the network.

c. In a Command Prompt window, ping the default gateway to test the connectivity to the default gateway address that was identified Part 2, Step 1.

```
C:\Users\Student> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 4ms
```

d. Ping the IPv4 addresses of other PCs on the LAN that were provided to you by your team members.

   Note: If your team member's PC does not reply to your pings, this may be because their PC firewall is blocking these requests. Ask your instructor for assistance to disable the PC firewall if necessary.

e. Stop capturing data by clicking **Stop Capture** (red square icon) on the toolbar.

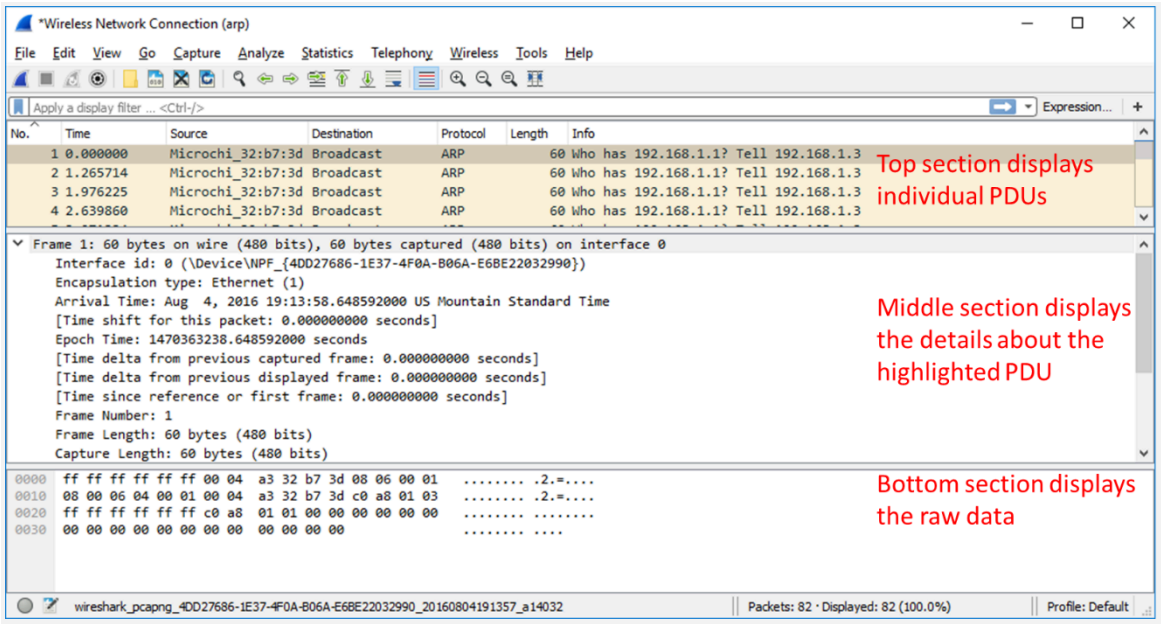
Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the **ping** requests of your team member's PC. Wireshark data is displayed in three sections:

1) The top section displays the list of PDU frames captured with a summary of the IPv4 packet information listed.

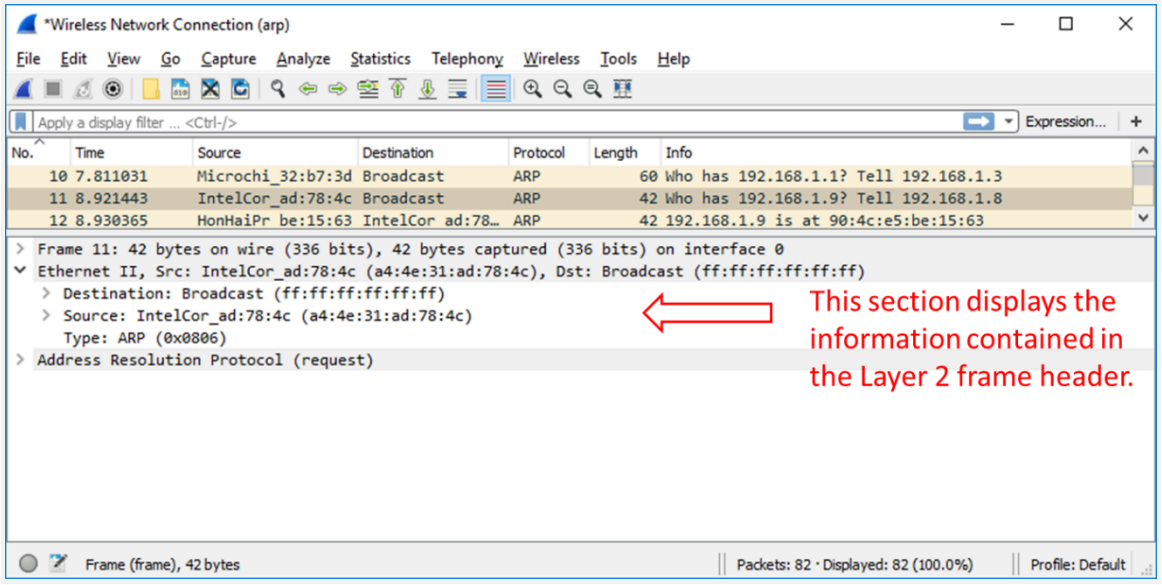
2) The middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers.

3) The bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.



a. Click one of the ARP frames in the top section that has your PC MAC address as the source address in the frame and “broadcast” as the destination of the frame.

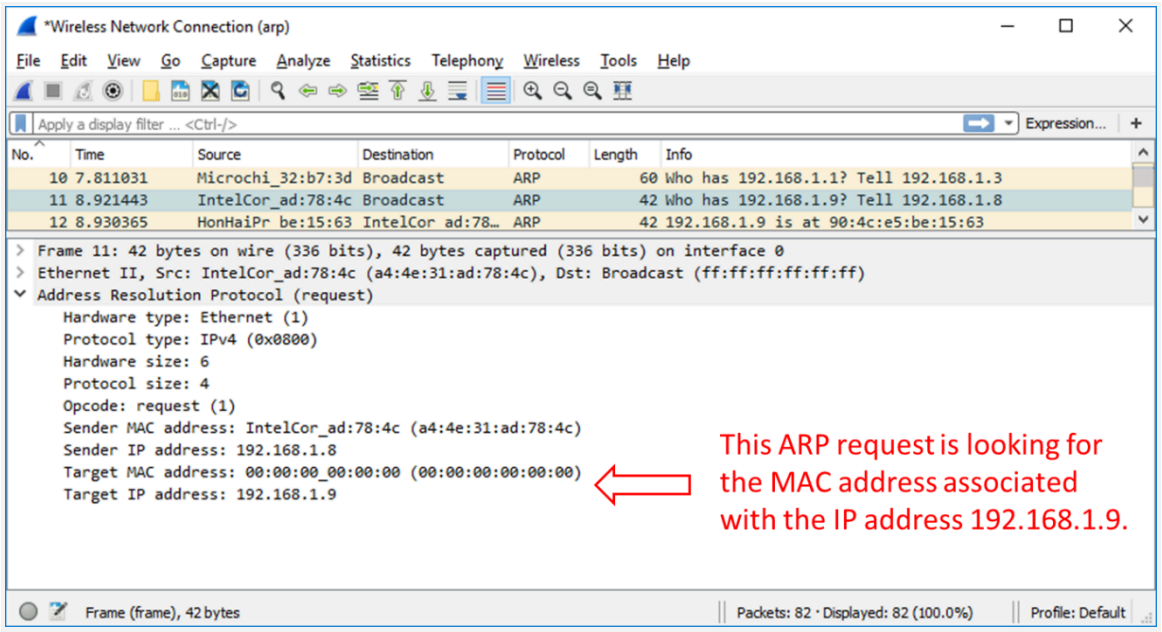
b. With this PDU frame still selected in the top section, navigate to the middle section. Click the arrow to the left of the Ethernet II row to view the Destination and Source MAC addresses.



Does the Source MAC address match your PC’s interface?

No

b. Click the arrow to the left of the Address Resolution Protocol (request) row to view the content of the ARP request.



Step 4: Locate the ARP response frame that corresponds to the ARP request that you highlighted.

a. Using the Target IPv4 address in the ARP request, locate the ARP response frame in the upper section of the Wireshark capture screen.

What is the IPv4 address of the Target device in your ARP request?

192.168.86.1

b. Highlight the response frame in the upper section of the Wireshark output. You may have to scroll the window to find the response frame that matches the Target IPv4 address identified in the previous step. Expand the Ethernet II and Address Resolution Protocol (response) rows in the middle section of the screen.

Is the ARP response frame a broadcast frame?

No

What is the destination MAC address of the frame?

(cc:f4:11:36:db:e9)

Is this the MAC address of your PC?

No

What MAC address is the source of the frame

(ac:fd:ce:1b:a2:e7)

c. Verify with your team member that the MAC address matches the MAC address of their PC.

Part 3: Examine the ARP cache entries on the PC.

After the ARP reply is received by the PC, the MAC Address to IPv4 address association is stored in cache memory on the PC. These entries will stay in memory for a short period of time (from 15 to 45 seconds), then, if they are not used within that time, they will be removed from cache.

a. Open a command prompt window on the PC. At the prompt, enter **arp –a** and press enter.

```
C:\Users\Student> arp -a

Interface: 192.168.1.8 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           00-37-73-ea-b1-7a     dynamic
  192.168.1.9           90-4c-e5-be-15-63     dynamic
  192.168.1.13          a4-4e-31-ad-78-4c     dynamic
  224.0.0.5             01-00-5e-00-00-05     static
  224.0.0.6             01-00-5e-00-00-06     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

The output of the **arp –a** command displays the entries that are in the cache on the PC. In the example, the PC has entries for the default gateway (192.168.1.1) and for two PCs that are located on the same LAN (192.168.1.9 and 192.168.1.13).

What is the result of executing the **arp –a** command on your PC?

This command displays the ARP (Address Resolution Protocol) table on your computer. The ARP table maps IP addresses to physical MAC (Media Access Control) addresses on the local network.It is useful for diagnosing network issues, checking for duplicate IP addresses, and identifying devices on the local network.

b. The **arp** command on the Windows PC has another functionality. Enter **arp /?** at the command prompt and press enter. The **arp** command options enable you to view, add and remove ARP table entries if necessary.

Which option deletes an entry from the ARP cache?

arp -d

What would be the result of issuing the **arp –d *** command?

This command on the PC would delete all entries in the ARP (Address Resolution Protocol) table. This action clears the ARP cache, which temporarily stores mappings of IP addresses to MAC addresses for devices on the local network.

Reflection

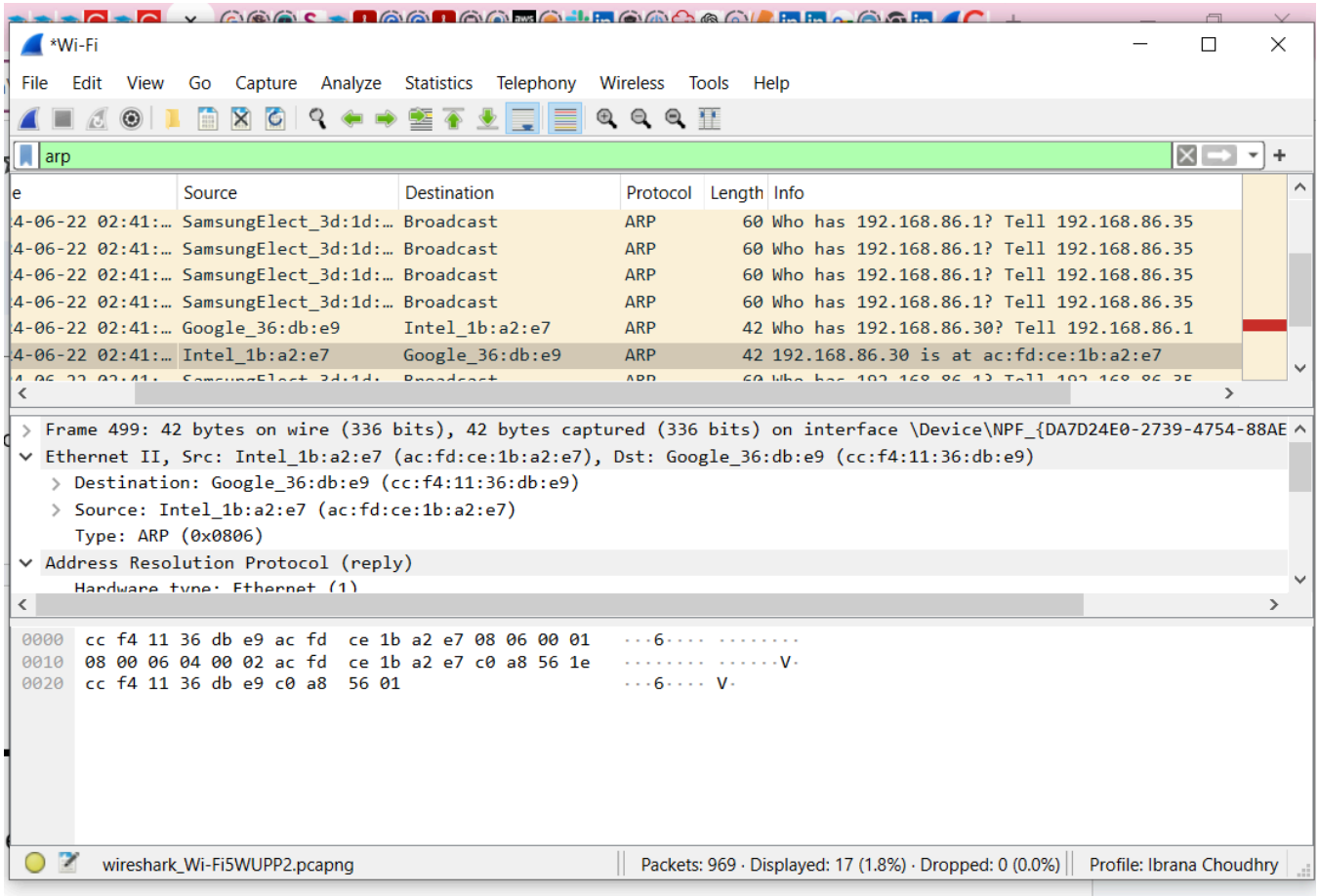
1. What is a benefit of keeping ARP cache entries in memory on the source computer?

   Reduced Network Traffic, Faster Communication, Improved Efficiency, Enhanced Network Performance and Optimized Resource Utilization.

   Maintaining an ARP cache in memory on the source computer is crucial for network efficiency and performance. It allows for quick resolution of IP addresses to MAC addresses, minimizes network traffic, and ensures faster and more reliable communication. This optimization is especially beneficial in environments with high traffic volumes and frequent inter-device communication.

2. If the destination IPv4 address is not located on the same network as the source host, what MAC address will be used as the destination target MAC address in the frame?

   When the destination IPv4 address is not located on the same network as the source host, the MAC address that will be used as the destination target MAC address in the frame is the MAC address of the default gateway (router) on the source host's local network.



MAC address matches the MAC address of their PC.