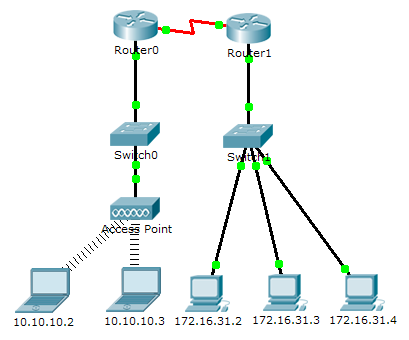
Notes:

1. This document contains the instruction and questions that you need to answer for the Packet Tracer activity named wk4-computer-prac-PKA-c-Examine-ARP-Table.pka.
2. Make sure you have downloaded and opened the Packet Tracer activity file named wk4-computer-prac-PKA-c-Examine-ARP-Table.pka.
3. Follow the instruction in this Word document to complete the Packet Tracer activity
4. Type in your answer to EACH question (highlighted) included in this document, immediately after the question in the space provided
5. Save this Word document and submit it as part of your Week 4 Computer Practical submission.

****Packet Tracer - Examine the ARP Table****

Topology



Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | MAC Address | Switch Interface |
| Router0 | Gig0/0 | 0001.6458.2501 | Gig1/1 |
| Se0/0/0 | N/A | N/A |
| Router1 | Gig0/0 | 00E0.F7B1.8901 | Gig1/1 |
| Se0/0/0 | N/A | N/A |
| 10.10.10.2 | Wireless | 0060.2F84.4AB6 | Fa0/2 |
| 10.10.10.3 | Wireless | 0060.4706.572B | Fa0/2 |
| 172.16.31.2 | Fa0 | 000C.85CC.1DA7 | Fa0/1 |
| 172.16.31.3 | Fa0 | 0060.7036.2849 | Fa0/2 |
| 172.16.31.4 | Gig0 | 0002.1640.8D75 | Fa0/3 |

Objectives

Part 1: Examine an ARP Request

Part 2: Examine the ARP Process in Remote Communications

Background

Recall that every device with an IP address on an Ethernet network also has an Ethernet MAC address. When a device sends an Ethernet frame, it contains these two addresses:

* Destination MAC address - The MAC address of the Ethernet NIC, which will be either the MAC address of the final destination device or the router.
* Source MAC address - The MAC address of the sender’s Ethernet NIC.

To determine the destination MAC address, the device uses **ARP** (**A**ddress **R**esolution **P**rotocol). ARP provides two basic functions:

* Resolving IPv4 addresses to MAC addresses
* Maintaining a table of mappings

When a packet is sent from the IP layer to the data link layer (of the same device) to be encapsulated into an Ethernet frame, the device refers to a table in its memory to find the MAC address that is mapped to the IPv4 address. This table is called the **ARP table** or the **ARP cache**. The ARP table is stored in the RAM of the device.

Each entry, or row, of the ARP table binds an IPv4 address with a MAC address. We call the relationship between the two values a map - it simply means that you can locate an IPv4 address in the table and discover the corresponding MAC address. The ARP table temporarily saves (caches) the mapping for the devices on the LAN.

The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address. When a host’s IP layer creates a packet for a destination, it compares the destination IPv4 address and its own IPv4 address to determine if the two IP addresses are located on the same Layer 3 network. Therefore, there are two possible scenarios with the search of the ARP table:

* If the packet’s destination IPv4 address is on the same network as the source IPv4 address, the device will search the ARP table for table entry with the destination IPv4 address and the corresponding MAC address.
* If the destination IPv4 address is on a remote network than the source IPv4 address, the device will search the ARP table for the table entry with the IPv4 address of the default gateway (interface of the local router) and the corresponding MAC address, as the source device needs to send the frame to its default gateway for the frame to be sent out of the local network.

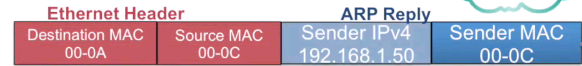
If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame. If there is no entry is found, then the device sends an ARP request.

An ARP request messages is encapsulated directly within an Ethernet frame. The ARP request message (encapsulated within an Ethernet frame) would look like the following, where Target Ipv4 is the IP address to be “resolved”, i.e. the ARP request is used to find the MAC address corresponding to the Target IP address.



Because ARP requests are broadcasts, they are flooded out all ports by the switch except the receiving port. All Ethernet NICs on the LAN process broadcasts. Every device must process the ARP request to see if the target IPv4 address matches its own. A router will not forward broadcasts out other interfaces.

Only one device on the LAN will have an IPv4 address that matches the target IPv4 address in the ARP request. All other devices will not reply. An ARP reply (encapsulated in an Ethernet frame) would look like:



When the ARP reply is received by the device who initiated the ARP request, the devices adds the mapping of the IP address and MAC address received in its ARP table.

1. Examine an ARP Request
   1. Generate ARP requests by pinging 172.16.31.3 from 172.16.31.2.
      1. Click **172.16.31.2** and open the **Command Prompt**.
      2. Enter the **arp -d** command to clear the ARP table.
      3. Enter **Simulation** mode and enter the command **ping 172.16.31.3**. Two PDUs will be generated. The **ping** command cannot complete the ICMP packet without knowing the MAC address of the destination. So the computer sends an ARP broadcast frame to find the MAC address of the destination.
      4. Click **Capture/Forward** *once*. The ARP PDU moves to **Switch1** while the ICMP PDU disappears, waiting for the ARP reply. Open the ARP PDU and record the destination MAC address. Is this address listed in the Addressing table on page 1?

Your answer: No, it’s not. It appeared the destination MAC address as ffff.ffff.ffff, which means broadcast address.

* + 1. Click **Capture/Forward** *once* to move the PDU to the next device. How many copies of the PDU did **Switch1** make?

Your answer: 3, to Router1, 172.16.31.3 and 172.16.31.4

* + 1. What is the IP address of the device that accepted the PDU?

Your answer:172.16.31.3

* + 1. Open the PDU and examine Layer 2. What happened to the source and destination MAC addresses?

Your answer: In Outbound PDU details

- the destination MAC address changed from ffff.ffff.ffff.ffff to 000C.85CC.1DA7

- the source MAC address changed from 000C.85CC.1DA7 (new destination address) to 0060.7036.2849

h. Click **Capture/Forward** until the PDU returns to **172.16.31.2**. How many copies of the PDU did the switch make during the ARP reply?

Your answer: There’s only one copy of the PDU that the switch had made during the reply

* 1. Examine the ARP table.
     1. Note that the ICMP packet reappears. Open the ICMP PDU and examine the MAC addresses. Do the MAC addresses of the source and destination align with their IP addresses?

Your answer: Yes, it is

* + 1. Switch back to **Realtime** and the ping completes.
    2. Click **172.16.31.2** and enter the **arp –a** command. To what IP address does the MAC address entry correspond?

Your answer: IP address: 172.16.31.3

* + 1. In general, when does an end device issue an ARP request? (**Hint**: refer to the **Background** section of the instruction of this lab for answer)

Your answer: When there is no entry is found, then the device will send an ARP request

1. Examine the ARP Process in Remote Communications
   1. Generate traffic to produce ARP traffic.
      1. Click **172.16.31.2** and open the **Command Prompt**.
      2. Enter the **ping 10.10.10.1** command.
      3. Type **arp –a**. What is the IP address of the new ARP table entry?

Your answer: There’re 2 IP addresses, one is 172.16.31.3, which is displayed previously in old table, and the other is 172.16.31.1.

* + 1. Enter **arp -d** to clear the ARP table and switch to **Simulation** mode.
    2. Repeat the ping to 10.10.10.1. How many PDUs appear?

Your answer: There’re two PDU appeared.

* + 1. Click **Capture/Forward** *once*. Click the PDU that is now at **Switch1**. What is the target IP address included in the ARP request?

Your answer: Target IP address: 172.16.31.1

* + 1. The target IP address is not 10.10.10.1. Why? (**Hint**: recall what’s stated in the Background section or shown in the 3rd video: When the destination of the communication (in this case, the Ping) is on a remote network, whose MAC address would the sending device request for using an ARP request message?)

Your answer: Because the destination IPv4 address is on a remote network, then the device will search the ARP table for the table entry with the IPv4 address of the default gateway and the corresponding MAC address, because the frame is needed to be sent to its default gateway in order to the frame could be sent out of the local network. i.e the device with IP address 10.10.10.1 and device with IP 172.16.31.2 are in two different local network.

* 1. Examine the ARP table on Router1.
     1. Switch to **Realtime** mode. Click **Router1** and then the **CLI** tab.

Enter privileged EXEC mode and then the **show mac-address-table** command. How many MAC addresses are in the table?

Your answer: There’s nothing in the table.

(**Note**: this command on a router means something completely different than the ‘show mac address-table’ used with a switch)

* + 1. Enter the **show arp** command. Is there an entry for **172.16.31.2**?

Your answer: Yes, it is