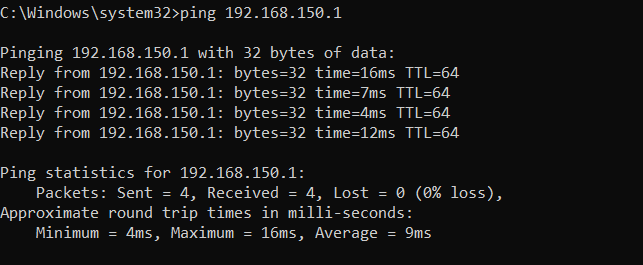
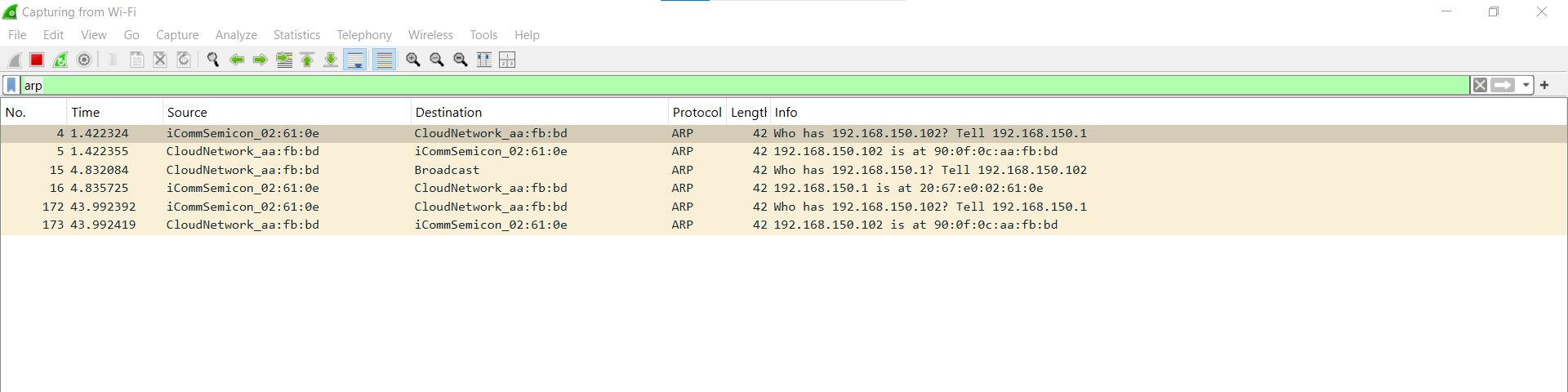
**1. Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address.**

**Discuss the importance of ARP in packet forwarding.**

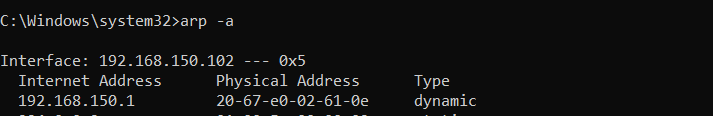
**Pinging 192.168.150.1**

****

**Capturing ARP:**

****

**ARP Table:**

****

**ARP Request and Reply Details**

**ARP Request:**

* Source MAC: iCommSemicon\_02:61:0e
* Source IP: 192.168.150.1
* Destination MAC: Broadcast (ff:ff:ff:ff:ff:ff)
* Destination IP: 192.168.150.102
* Opcode: Request (1)
* Message: "Who has 192.168.150.102? Tell 192.168.150.1"

**ARP Reply:**

* Source MAC: CloudNetwork\_aa:fb:bd
* Source IP: 192.168.150.102
* Destination MAC: iCommSemicon\_02:61:0e
* Destination IP: 192.168.150.1
* Opcode: Reply (2)
* Message: "192.168.150.102 is at 90:0f:0c:aa:fb:bd"

**Importance of ARP in Packet Forwarding:**

* Translates IP addresses to MAC addresses for local network communication.
* Essential for forwarding packets at the Data Link Layer (Layer 2).
* Helps devices find the router’s MAC address for forwarding packets outside the local network.
* Uses ARP requests and replies to update MAC addresses dynamically.
* Without ARP, devices wouldn’t know where to send packets, leading to communication failure.
* Maintains an ARP cache to reduce unnecessary broadcasts and improve efficiency.