WIRESHARK

ARŞ. GÖR. MELEK ŞENTÜRK

WHAT IS ARP?

ARP (Address Resolution Protocol) is a protocol used to determine the physical MAC address corresponding to an IP address of a device on a network.

A device needs to know the MAC address of the device it wants to communicate with. If it doesn't know this address, it sends an ARP request to learn the MAC address corresponding to the IP address.

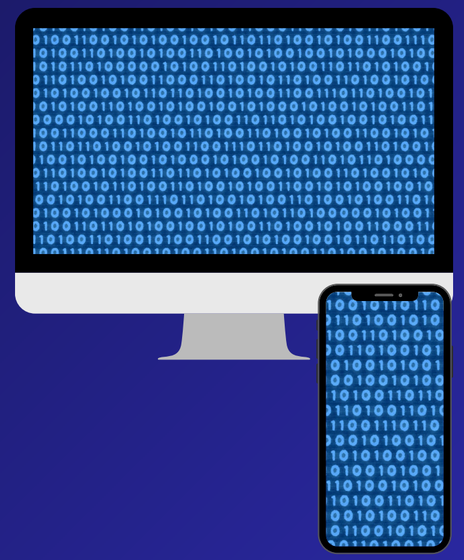
ARP Request and ARP Reply are the two main types of ARP packets.

THE DIFFERENCE BETWEEN IP AND MAC ADDRESS

An IP address is a device's logical address on a network and is typically used by routers.

A MAC address is a device's physical address and is the unique identity of the network interface card. These addresses are used for data transmission between devices on a local network.

HOW DOES IT WORK?



If the device does not know the MAC address for the target IP:

It broadcasts an ARP Request packet (Broadcast - "Send to everyone").

The packet contains the information, "Who owns this IP address? Tell me the MAC address!"

The target device responds:

The target device sends an ARP Reply packet, providing its MAC address.

The response is sent only to the device that made the request (Unicast).

The MAC address is saved in the ARP table.

The device saves the MAC address in the ARP cache, so it doesn't need to send an ARP request for each request.

The ARP cache is cleared after a certain period of time.

ARP'S SECURITY VULNERABILITIES AND ATTACK METHODS

ARP Spoofing / ARP Poisoning:

An attacker can send false ARP replies, impersonating themselves as a device on the network.

For example, the attacker can say "I am the router" and redirect traffic to their own device.

Man-in-the-Middle (MitM) Attacks:

With ARP spoofing, the attacker can intercept traffic between two devices on the network and eavesdrop.

ARP TABLE

By using the "arp -a" command, we can view the IP-MAC mappings in the ARP table.

```
PS C:\WINDOWS\system32> arp -a

Interface: 192.168.1.101 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           4c-d6-29-60-52-71     dynamic
  192.168.1.115         e8-5a-8b-b9-f1-e4     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

INITIATING AN ARP REQUEST

Firstly, to reset the connections in the ARP table:

We will reset the IP-MAC mappings in the ARP table and initiate a new ARP request.

```
PS C:\WINDOWS\system32> netsh interface ip delete arpcache
Ok.

PS C:\WINDOWS\system32> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms 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 = 2ms, Maximum = 3ms, Average = 2ms
PS C:\WINDOWS\system32>
```

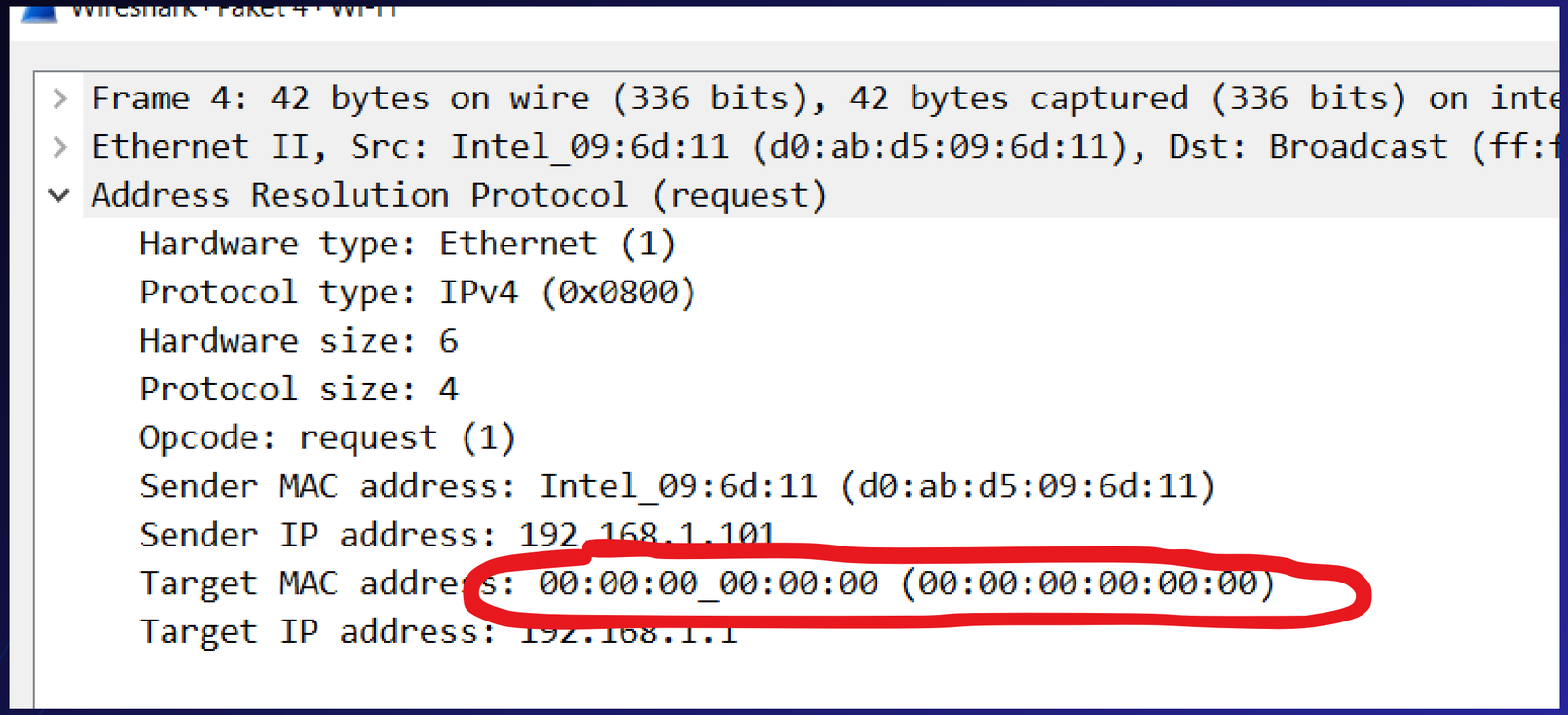
WIRESHARK SIDE

Source	Destination	Protocc	Length	Info
Intel_09:6d:11	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.101
HuaweiTechno_60:…	Intel_09:6d:11	ARP	42	192.168.1.1 is at 4c:d6:29:60:52:71

The ARP request was broadcast to the entire network. All devices on the network can respond to this broadcast, but only the device with the IP address 192.168.1.1 will reply.

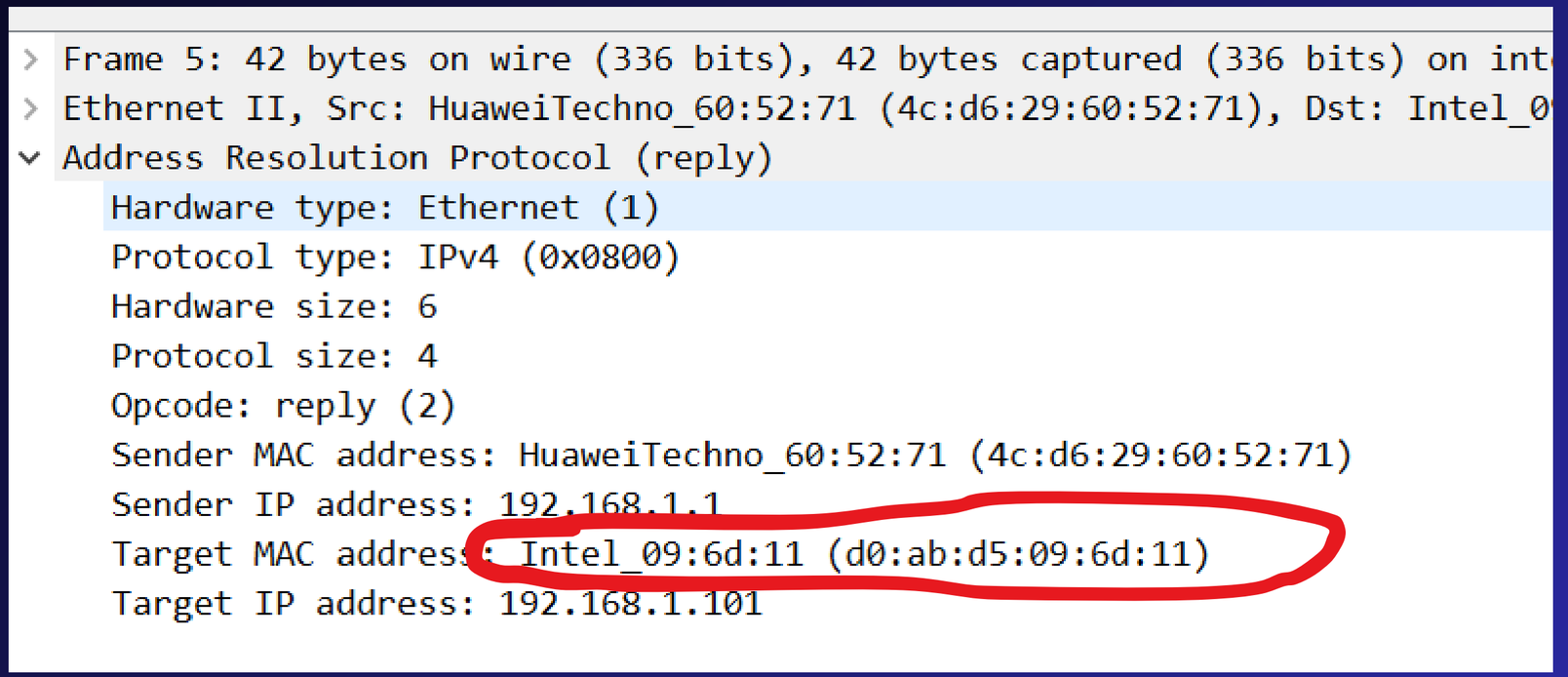
The device with the IP address 192.168.1.1 (modem/router) responds by providing its MAC address. It says, "My MAC address is 4c:d6:29:60:52:71." This response is sent only to the computer that made the request (192.168.1.101), as ARP replies are transmitted via unicast.

ARP REQUEST CONTENT



The ARP request is only for MAC-IP mapping. Since no data is transferred, there is no TCP/UDP. As no application is used (HTTP, FTP, DNS, etc.), they are not present.

ARP REQUEST CONTENT



The MAC address of the target IP has been returned.

THE LOGIC OF ARP SPOOFING.

By manipulating this process, we can send fake ARP replies to devices on the network. For this:
Let's assume the target device is 192.168.1.101 and the router has the IP address 192.168.1.1. We send a fake ARP reply to the target device (192.168.1.101), saying "I am the router (192.168.1.1), and my MAC address is [attacker's MAC address]." Similarly, we send a fake ARP reply to the router, saying "I am 192.168.1.101, and my MAC address is [attacker's MAC address]." The target device sends all its data to the attacker's MAC address because it thinks it's the router. The router also sends the target device's data to the attacker's MAC address. The attacker can then intercept, modify, or forward this traffic on their device.