WIRESHARK

Res. Asst. Melek ŞENTÜRK

What is DHCP?

- **DHCP (Dynamic Host Configuration Protocol),**
    - It is a protocol that allows network devices (phone, computer, tablet, etc.) to automatically obtain IP addresses and network settings (Subnet Mask, Gateway, DNS).
- **Main Purpose,**
    - When devices connect to the network, they do not have to make IP settings.
    - The network administrator does not need to manually assign IP to each device.
    - Error cases are minimized.

WHAT DOES DHCP PROTOCOL DO?

- **Automatic IP Assignment**
    - Devices automatically obtain IP and network settings.
- **Managing Network Traffic**
    - IP usage becomes more organized and conflicts are prevented.
- **Speed and Convenience**
    - Devices connect quickly in large networks without manual adjustments.
- **Flexibility**
    - As the network expands, new devices can easily get IP.

HOW DOES DHCP PROTOCOL WORK?

- **Discover:**
  - When a device first joins the network, it does not have an IP.
  - Broadcast sends message: “Is there a DHCP server that can give me an IP?”
- **Offer:**
  - The DHCP server replies: “I offer you the IP address 192.168.1.50.”
  - As the network expands, new devices can easily get IP.
- **Request:**
  - The device accepts the offer and says, “I want this IP!”
  - As the network expands, new devices can easily get IP.
- **Acknowledge (ACK):**
  - The DHCP server confirms the request: “Your IP address is now yours.”

WHAT İS THE ROLE OF A MODEM?

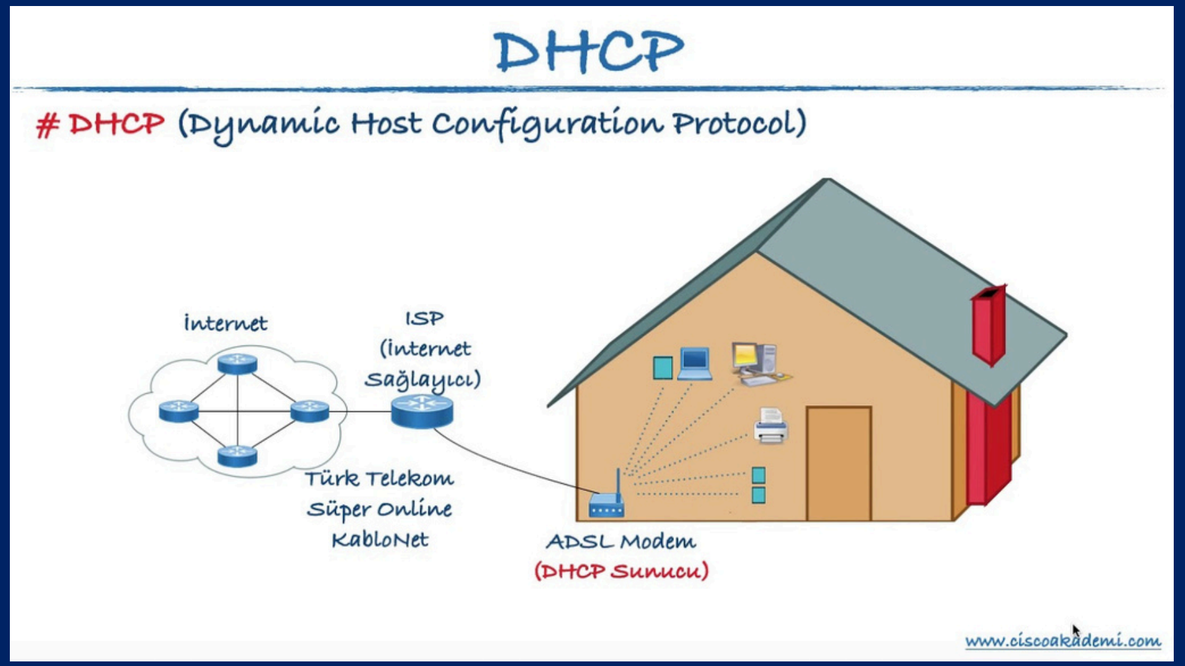
- **WAN (Wide Area Network) Side:**
    - The modem connects to the service provider's (ISP) network.
    - Usually, it logs in with username and password via PPPoE protocol or obtains a public IP automatically via DHCP.
    - Obtains a Public IP address from the ISP (e.g. 85.105.15.23).
- **LAN (Local Area Network) Side:**
    - The modem acts as a DHCP server for devices in the home (phones, computers).
    - It distributes private IP addresses (such as 192.168.1.10) to devices.
    - By performing NAT (Network Address Translation), it exposes many devices in the internal network to the internet via a single Public IP in the outside world.

MODEM AND DHCP RELATİONSHİP

- **The modem works as a DHCP server on the LAN side:**
  - Devices receive IP, Gateway and DNS settings via the modem's DHCP service.

- **The modem acts as a DHCP client on the WAN side:**

- It gets a Public IP for itself from the ISP.



WHAT İS DHCP FLOODİNG?

- DHCP Flooding means sending a large number of fake DHCP Discover messages on a network.

- Many more DHCP requests are created than would normally be the case.

- **Purpose: to overload, occupy, or render the DHCP server on the network inoperable.**

HOW DOES DHCP FLOODİNG WORK?

- Normally a device:
    - Sends 1 DHCP Discover.
    - Gets an IP address → job done.

- But an attacker who performs a DHCP Flood:
    - It sends thousands of fake DHCP Discover packets.
    - It uses fake MAC address in each packet (makes it look like different device).

Because the DHCP server must allocate a new IP address for each different MAC address.

The DHCP server's IP pool is full.

Real devices on the network can no longer get an IP.

WHAT HAPPENS TO THE NETWORK WHEN DHCP FLOOD OCCURS?

- Real users cannot connect to the network:
(Gives "Unable to obtain IP address" error.)

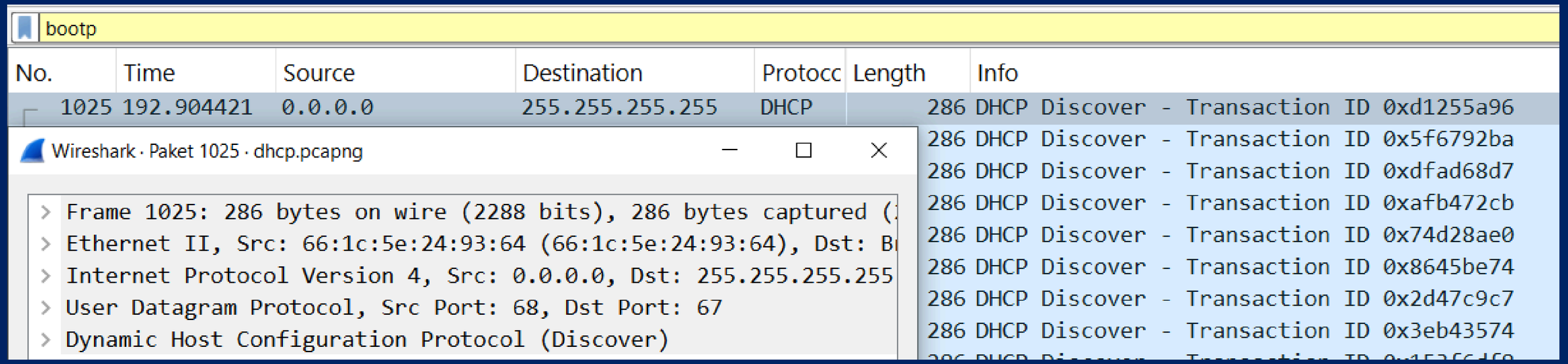
- Heavy traffic occurs on the network:
(DHCP server is overworked, CPU and RAM usage increases.)

- Internet access is cut off:
(Since there is no IP, you cannot connect to the internet.)

- Some of the systems on the network crash:
(Devices such as switches and routers can also be overloaded.)

WIRESHARK SİDE

- We can observe it on Wireshark by performing a DHCP flood attack. The Python “scapy” library can be used for the attack.



WIRESHARK SİDE

- Since there are fake DHCP requests, each request's MAC address is introduced differently. In fact, the MAC addresses shown are not correct.

```
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: 66:1c:5e:24:93:64 (66:1c:5e:24:93:64)
```

```
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: 82:6a:ab:84:65:c0 (82:6a:ab:84:65:c0)
```

```
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: d8:fd:08:c6:e1:19 (d8:fd:08:c6:e1:19)
```