DHCP Starvation Attack Problem

Application Layer: L2, L3

Description:

DHCP Starvation is a type of DoS (Denial of Service) attack that aims to completely exhaust the IP address pool of the DHCP server on the network with spoofed requests. This attack occurs when an anonymous or malicious user/attacker on the network sends successive DHCPDISCOVER messages to the DHCP server, pretending to be hundreds of clients with forged MAC addresses.

How the Attack Works:

In the normal state, when a DHCP client is connected to the network:

Sends a -DHCPDISCOVER message.

-The server responds with DHCPOFFER.

-IP is assigned, the client works with the IP address.

In the Starvation scenario, the attacker:

-Using software (e.g. Yersinia, DHCPig, DHCPstarv)

-Continuously generates new fake MAC addresses over the network.

-With these MAC addresses, it acts like a new client each time and sends DHCPDISCOVER message repeatedly.

-The DHCP server allocates IP addresses for each incoming request and the IP pool fills up in a short time.

-No longer can the DHCP server issue IPs to new clients, because:

All IPs appear to be "rented".

Real users receive automatic, invalid IPs such as "APIPA (169.254.x.x)".

The DHCP protocol has no client authentication mechanism, so it assigns an IP address to every incoming request in good faith. This makes the protocol vulnerable to attacks.

No special hardware is required to carry out the attack; only software that can generate forged DHCP requests (for example: Yersinia, DHCPig, DHCPstarv).

Even if a single device is connected to a switch, it can consume the entire IP pool by generating forged MAC addresses, thus causing the entire network to be out of service.

Purpose of the Attack

Preventing real users from connecting to the network.

Creating a service interruption.

The next step is to make a MITM (Man-in-the-Middle) attack by setting up a fake DHCP server on the network.

DHCP Protocol Design and Vulnerabilities

Dynamic Host Configuration Protocol (DHCP) is a network protocol developed to automatically assign network configuration information such as IP address, subnet mask, default gateway, and DNS server to client devices. DHCP is based on the "first-come-first-served" logic and processes incoming requests without verification or authentication.

While this provides ease of configuration, the lack of authentication allows attackers to manipulate the system with forged requests. The protocol generates a response to every valid DHCPDISCOVER message and therefore has an attack surface.

Attacker's Vulnerability Exploitation Method: A malicious user generates a large number of fake MAC addresses with the help of special tools such as Yersinia, DHCPig, Scapy, dhcp-starv and creates a separate DHCPDISCOVER message for each of them. The server recognises these requests as different clients and allocates IP addresses for each of them. This process can be repeated hundreds of times in milliseconds. As a result, the DHCP server's pool of assignable IP addresses (for example 192.168.1.100-192.168.1.200) is quickly exhausted.

Impact: Exclusion of Real Users: If the IP pool is fully allocated, real clients wishing to connect to the network cannot obtain a valid IP address. These clients are configured with an invalid IP in the APIPA (169.254.x.x) range that the operating system automatically assigns. This prevents network connectivity from being established; users cannot access the Internet and local resources. The network administrator can observe that the DHCP server is full, but the vast majority of these IPs are assigned to bogus MAC addresses that do not actually exist. This creates a situation that makes detection and intervention difficult.

Symptoms - Observable Effects of a DHCP Starvation Attack

When a DHCP Starvation attack is successfully implemented, various symptoms are observed both on the client side and at the network management level. These symptoms reveal anomalies related to IP address allocation and disruption of network services.

-Real Clients Not Getting IP

When legitimate clients make IP requests to the DHCP server, the server cannot respond if the IP pool is completely exhausted. As a result

Devices are automatically assigned by operating systems with the address APIPA (169.254.x.x).

Network connection cannot be established, clients cannot join the network because DHCP response cannot be received.

-Interruption of Network Access / Connection Problems

Users cannot access the internet or intranet resources.

A "yellow exclamation mark" appears in the system tray.

The following error messages may occur in the scanner:

"Server unreachable"

"DNS server not responding"

"No network connection"

-Abnormalities in **DHCP** Server Logs

When DHCP logs are examined by the network administrator, the following situations can be observed:

An unusual number of DHCPDISCOVER messages were received in a short period of time.

IP is assigned to a large number of unique MAC addresses at the same time.

Most of the leased IP addresses are never used (IPs are not used by active devices).

MAC addresses of leased devices are not recognised.

`-ipconfig /all` Output on **Client** Devices

When clients run the `ipconfig /all` or `ifconfig` commands, output is obtained as follows:

```
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 169.254.41.73
Default Gateway . . . . . . . . . :
```

This output indicates that the device cannot obtain IP from the DHCP server and has assigned itself a temporary, non-routable address.

-Anomaly in MAC Table on Switch

When looking at the switch with the `show mac address-table` or similar command:

Hundreds of different, unknown MAC addresses may be registered.

Most of these MAC addresses belong to rogue clients that are not physically present on the network.

Problems such as MAC table overflow may occur in the network.

Admin Guide - Solution Steps

The following security configurations are recommended to prevent a DHCP Starvation attack. These steps can be implemented on Cisco IOS supported switches.

The methods described below:

-DHCP Snooping (blocks fake DHCP requests)

-Port Security (closes the port when there are too many requests from certain MAC addresses)

Step 1: Enable DHCP Snooping Feature

Objective:
DHCP Snooping inspects DHCP traffic and only accepts offers from trusted ports. Thus, the attacker's fake IP requests are blocked.

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
```

vlan 10 is the VLAN through which DHCP traffic passes. Enter the appropriate VLAN number for your environment.

Step 2: Define Trusted Ports (Trusted vs. Untrusted)

Trusted port → The port to which the DHCP server is connected (allowed)

Untrusted port → Ports to which client devices are connected (limited)

-Make the port of the DHCP Server Trusted:

```
Switch(config)# interface fa0/1
Switch(config-if)# ip dhcp snooping trust
```

-Set Rate Limiting on **All** Client Ports:

```
Switch(config)# interface range fa0/2 - 24
```

Switch(config-if-range)# ip dhcp snooping limit rate 5

The limit rate 5 command limits 5 DHCP packets per second per port. This prevents the attacker from sending hundreds of fake packets.

-Additional Reinforcement with **Port** Security

Objective:
To detect a potential attack when more than one MAC address is received on a port and disable the port.

Switch(config)# interface fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation shutdown

This configuration allows only 1 different MAC address from a client port. When the attacker sends fake MAC addresses, the switch closes the port.

Post-Configuration Tests

Validation Commands:

Switch# show ip dhcp snooping
Switch# show ip dhcp snooping binding
Switch# show port-security interface fa0/2
Switch# show interfaces status

-Ping test

The client should now be able to receive IP from DHCP and communicate.

Impact of Security Measures: With these configurations, the network can be protected against service-disrupting attacks such as DHCP Starvation. While real users are guaranteed to receive IP, attacker devices are prevented from consuming the IP pool.

Cisco Packet Tracer Simulation

OBJECTIVES:

-Demonstrate the normal operation of DHCP

-To show that the attacker has exhausted the IP pool with DHCPDISCOVER bombardment

-Proving that the legitimate client cannot receive IP (169.254.x.x receives)

Logic of Simulation

Device	Role Description
Switch	It is the central component that manages all traffic on the network. It delivers DHCP traffic to devices.
Server0	Provides DHCP service. It automatically assigns IP to clients from a specific IP pool.
PC0	Legitimate client. A normal user device that receives an IP from DHCP.
PC1	Attacker device. Misleads the DHCP server by using forged MAC addresses.

Vulnerable Network Environment Scenario

-Server0 activates the DHCP service and defines a specific IP pool (192.168.1.10-192.168.1.19).

-PC0 successfully obtains an IP via DHCP and connects to the network normally.

-PC1 (the attacker) pretends to be a large number of fake clients by changing the MAC address in each request.

-The DHCP server distributes the entire IP pool to rogue clients.

-No more real devices like PC0 can get IP from DHCP.

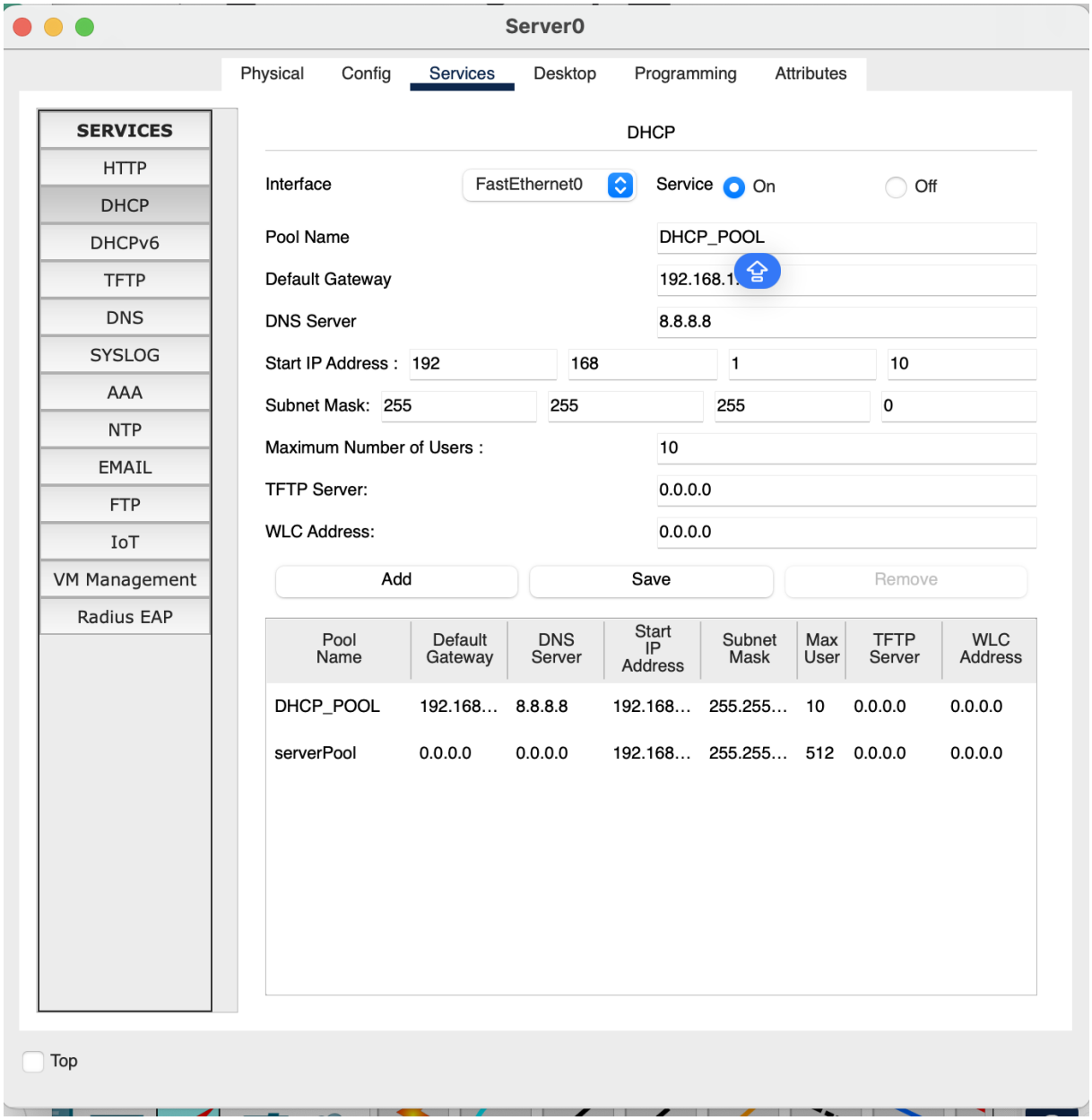
-169.254.x.x (APIPA) address starts to appear on real clients.

-Network communication crashes → DHCP Starvation attack is successfully performed.

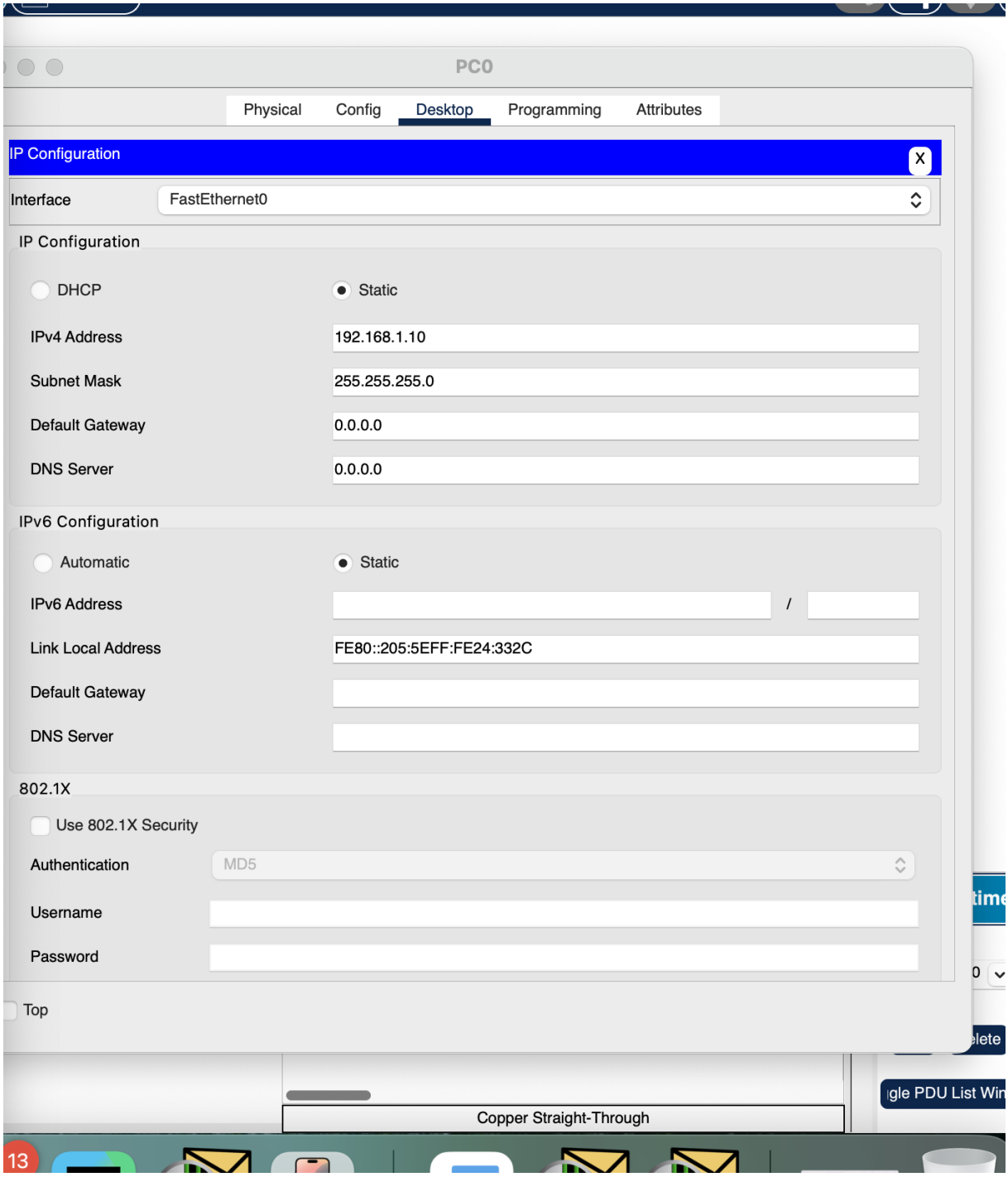
DHCP Starvation Attack - Simulation Explanation with Visuals

DHCP Service Setup on Server0 :

An IP pool has been defined for Server0, the DHCP server, and gateway and DNS have been determined. Automatic IP distribution is configured on the network.

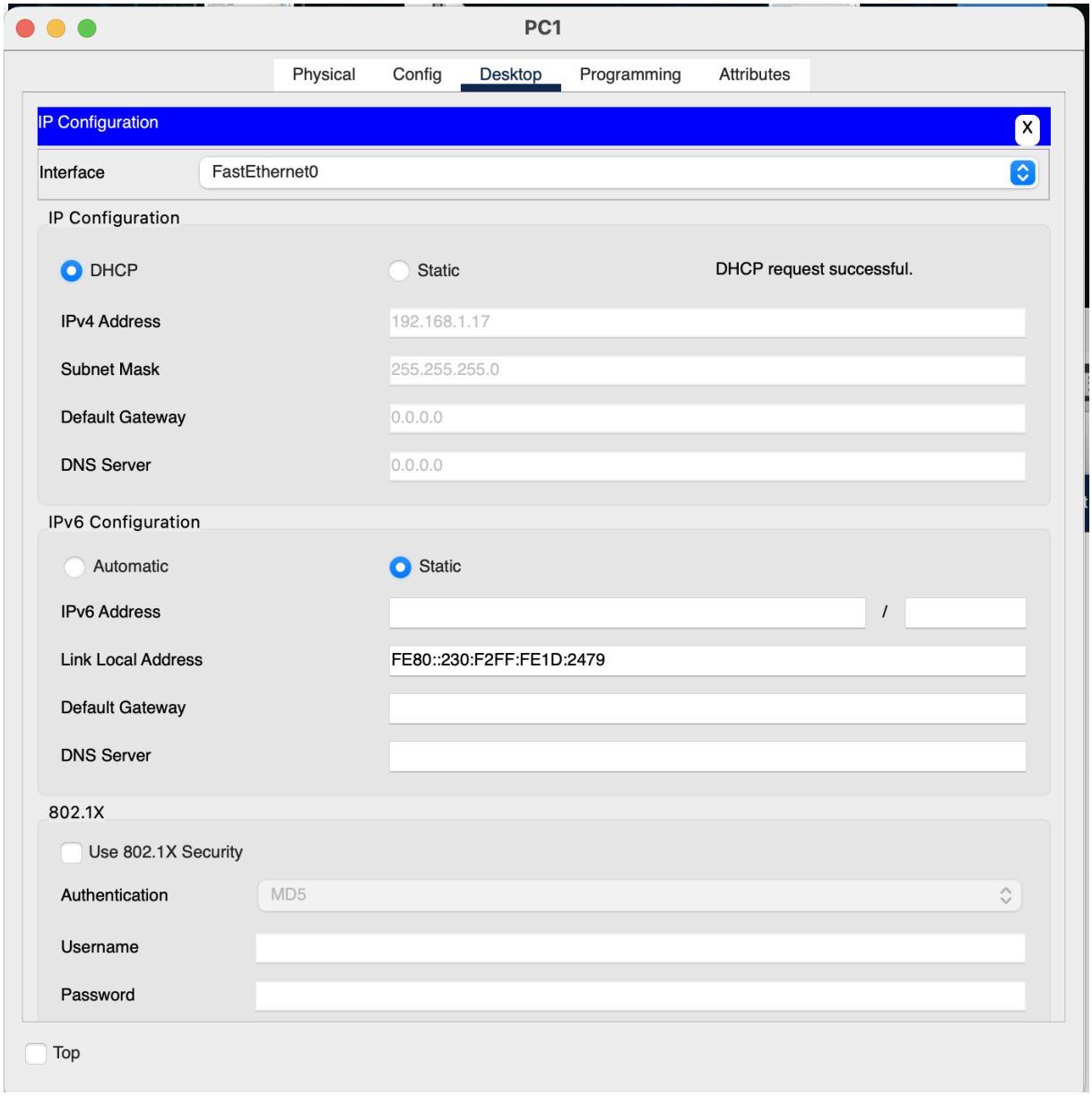


Attacker's MAC Address Noted:
The MAC address of the PC1 device that will perform the attack is displayed. The pool will be consumed by changing the MAC address for each new request

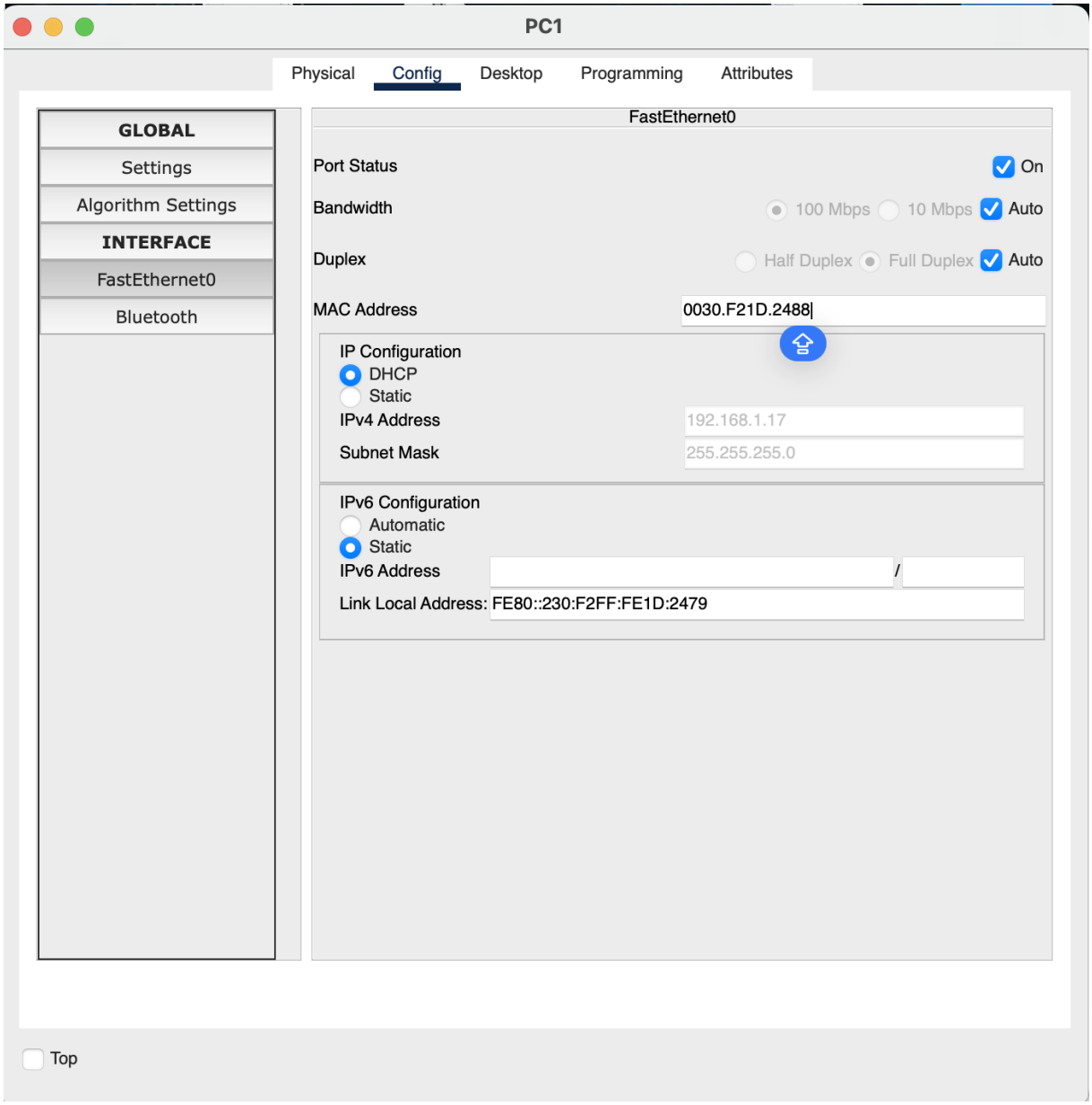


Static IP Defined PC:

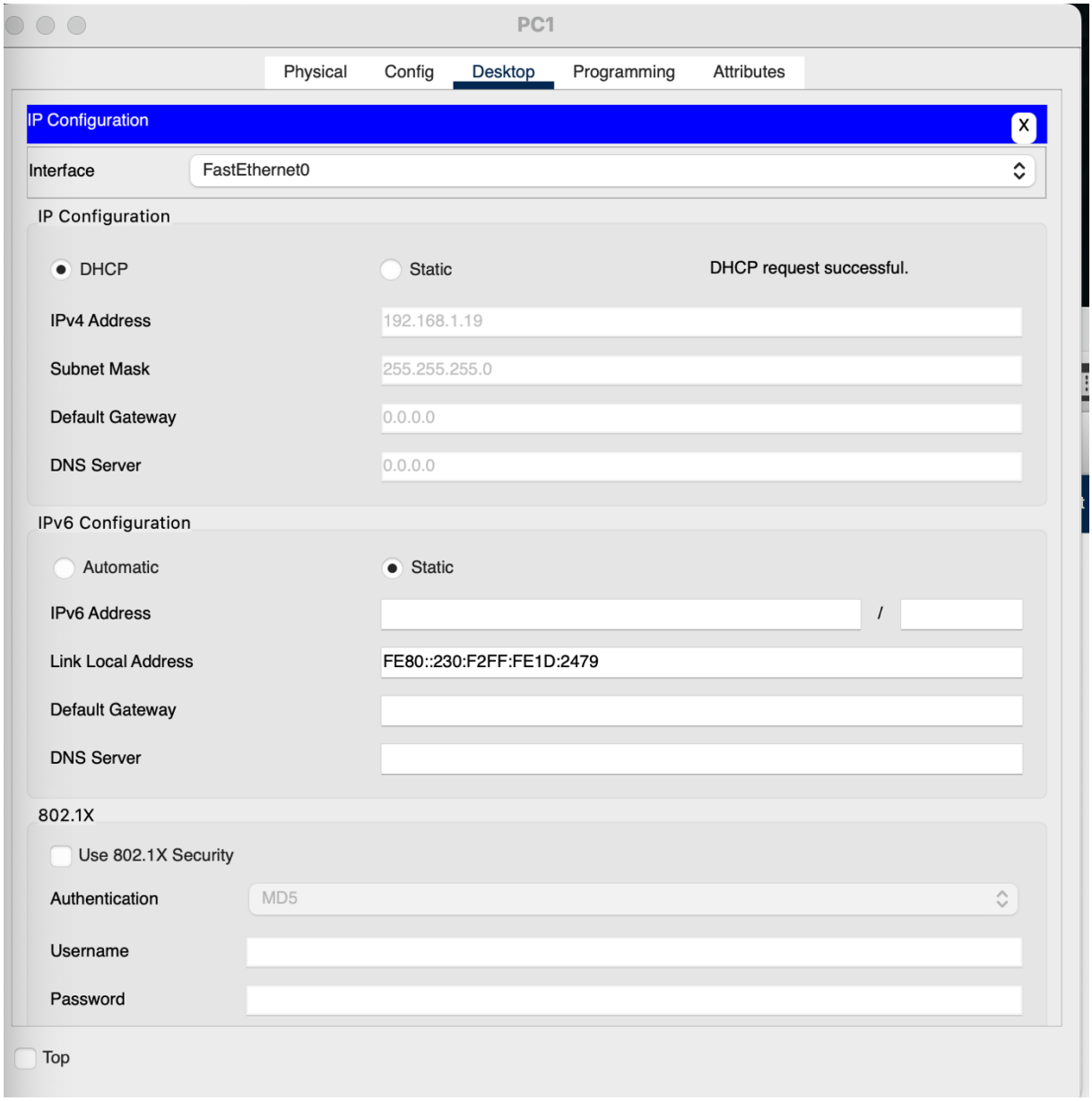
A device with a fixed IP (e.g. administrator PC) that will not be affected by the attack is shown. A device with a fixed address other than DHCP can be used for testing.



Innocent Device Successfully Obtaining IP from DHCP:
PC0, a normal client, can successfully obtain IP from DHCP. This is the normal state before the attack begins.

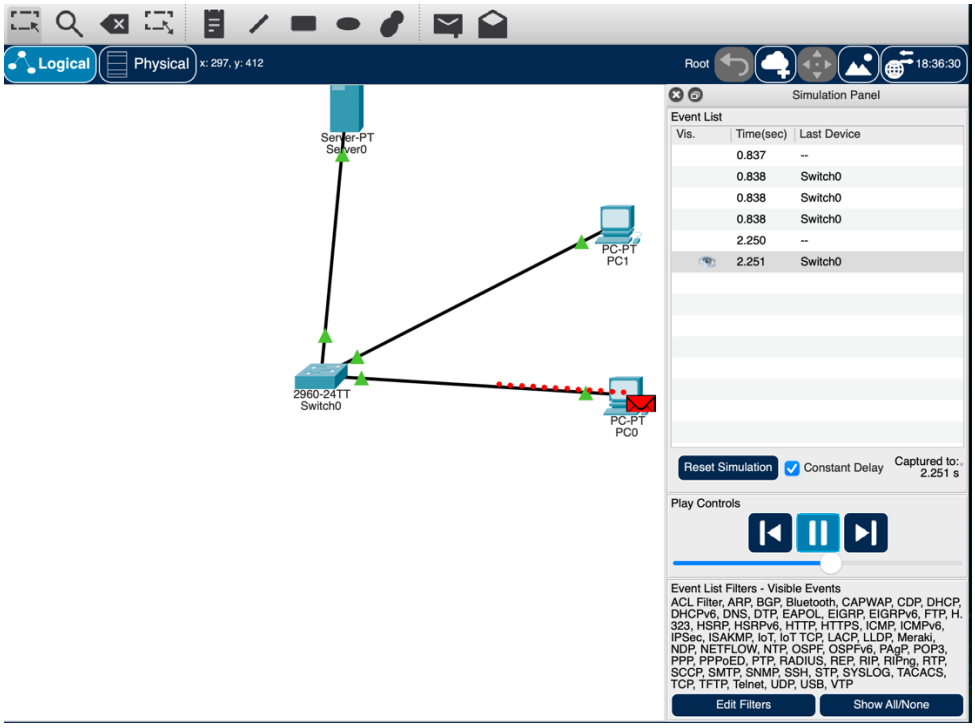


Attacker Changes MAC:
The attacker pretends to be a new client by changing the MAC address in each IP request, rapidly consuming the IP pool.



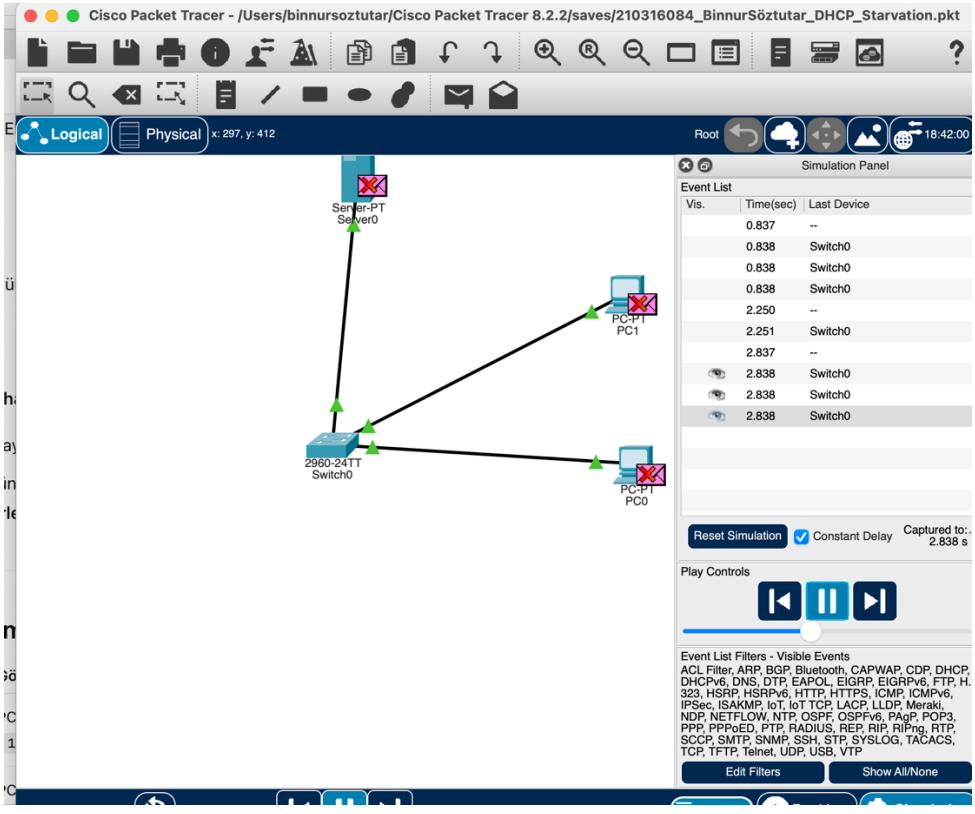
DHCP Starvation Begins:

When the simulation is started, DHCP packets are started to be sent by the attacker. Traffic density starts on the switch.



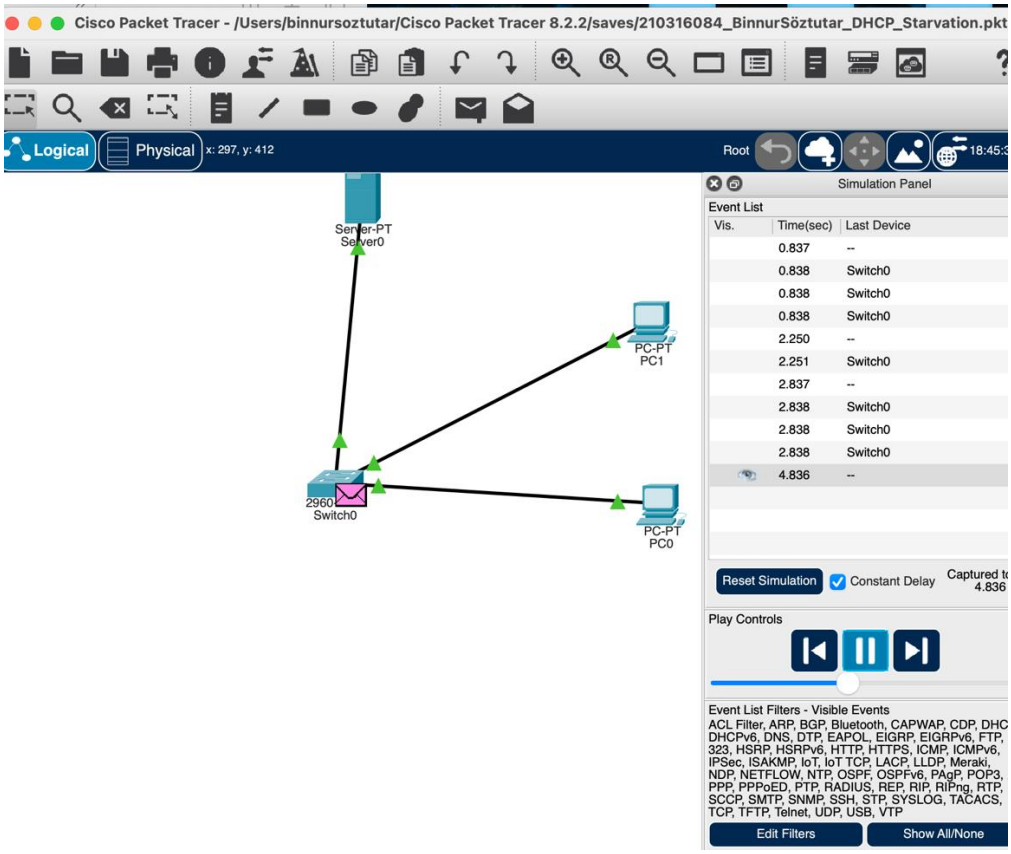
7.) Monitoring DHCP Traffic

Due to fake DHCPDISCOVER packets coming in continuously, there is heavy pink traffic on the ports on the switch



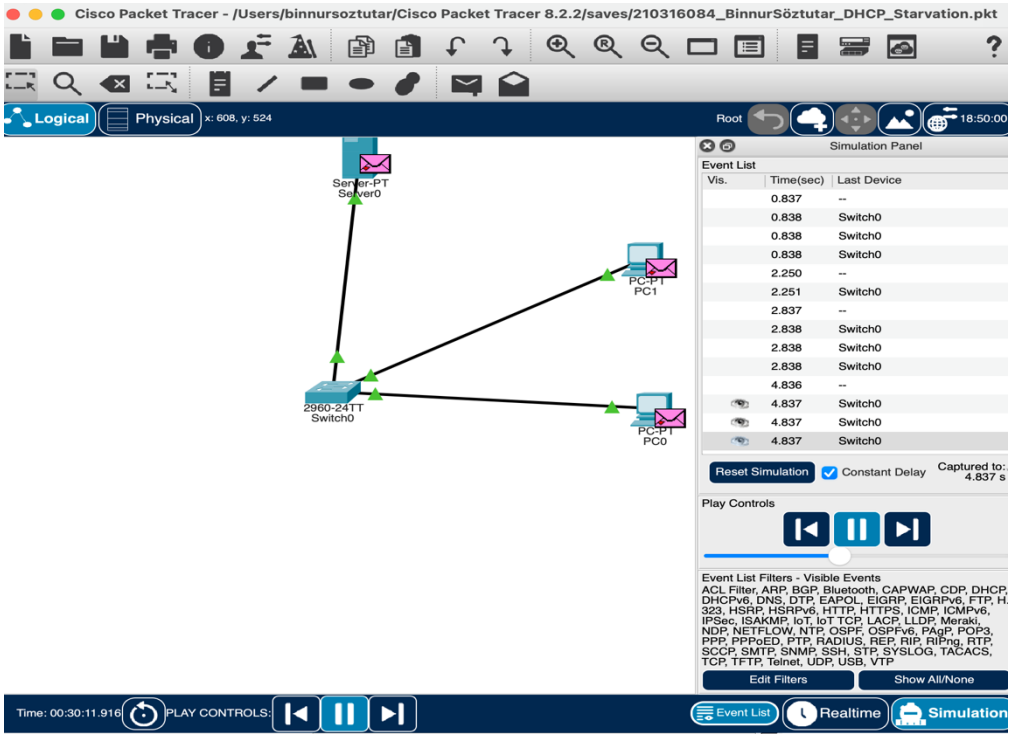
8.) Switch Responds to Traffic

The switch is under load when trying to route incoming DHCP requests.



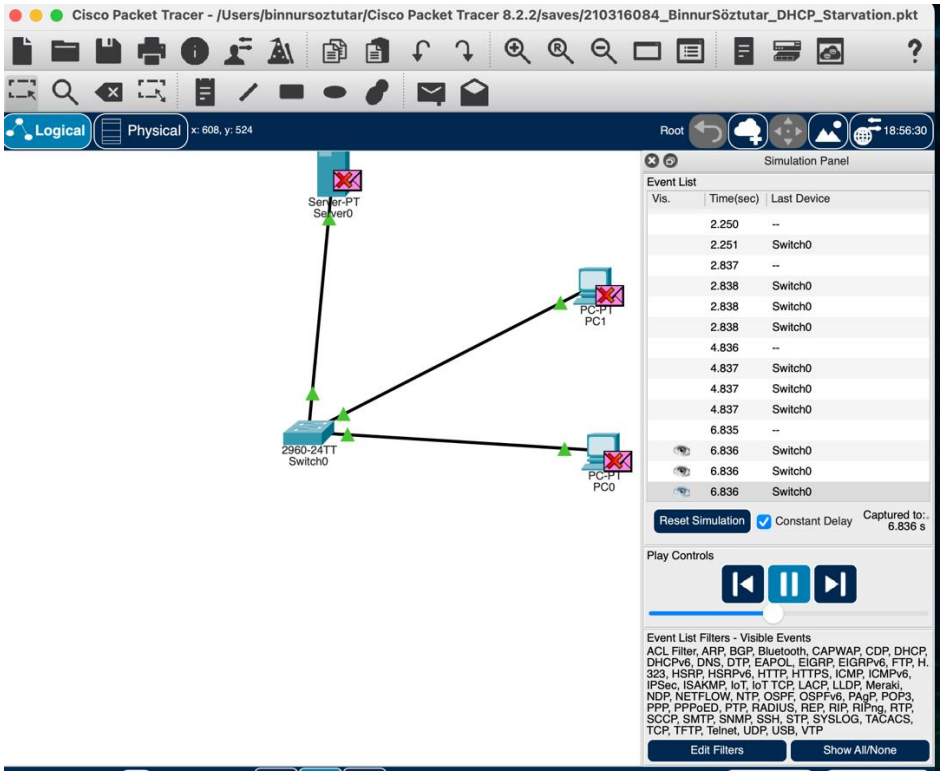
DHCP Traffic Cannot Reach Server:

As DHCP packets pass through the switch, some are lost or delayed. The server may be overloaded.



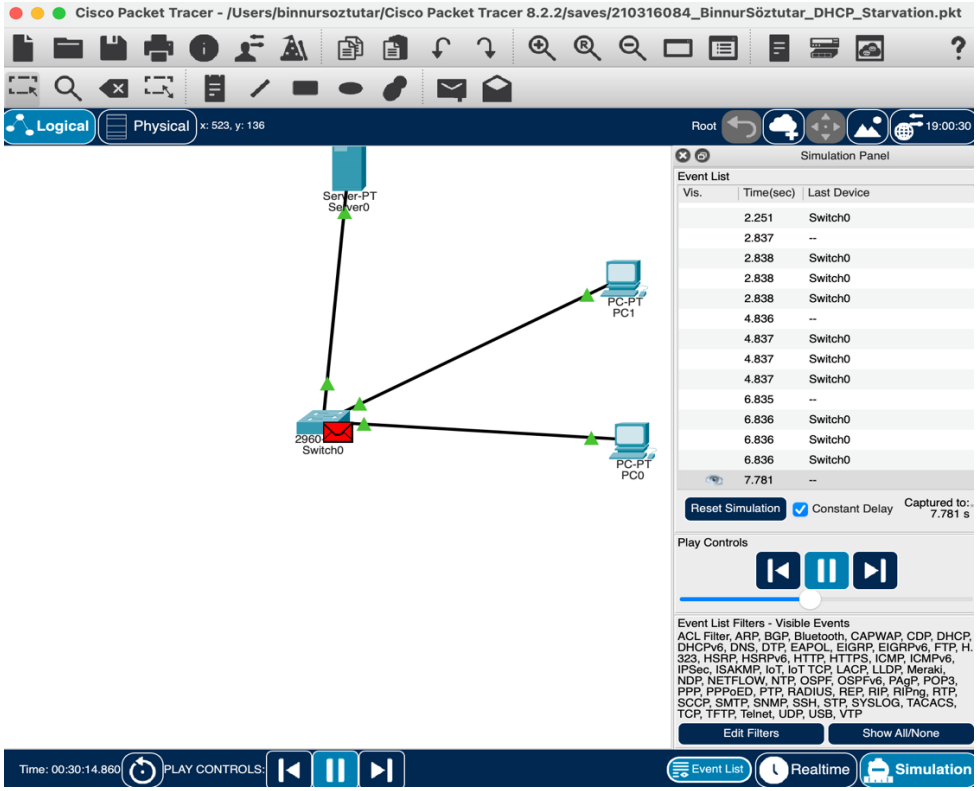
Congestion Started:

The IP pool is almost exhausted and request responses are delayed in the network.



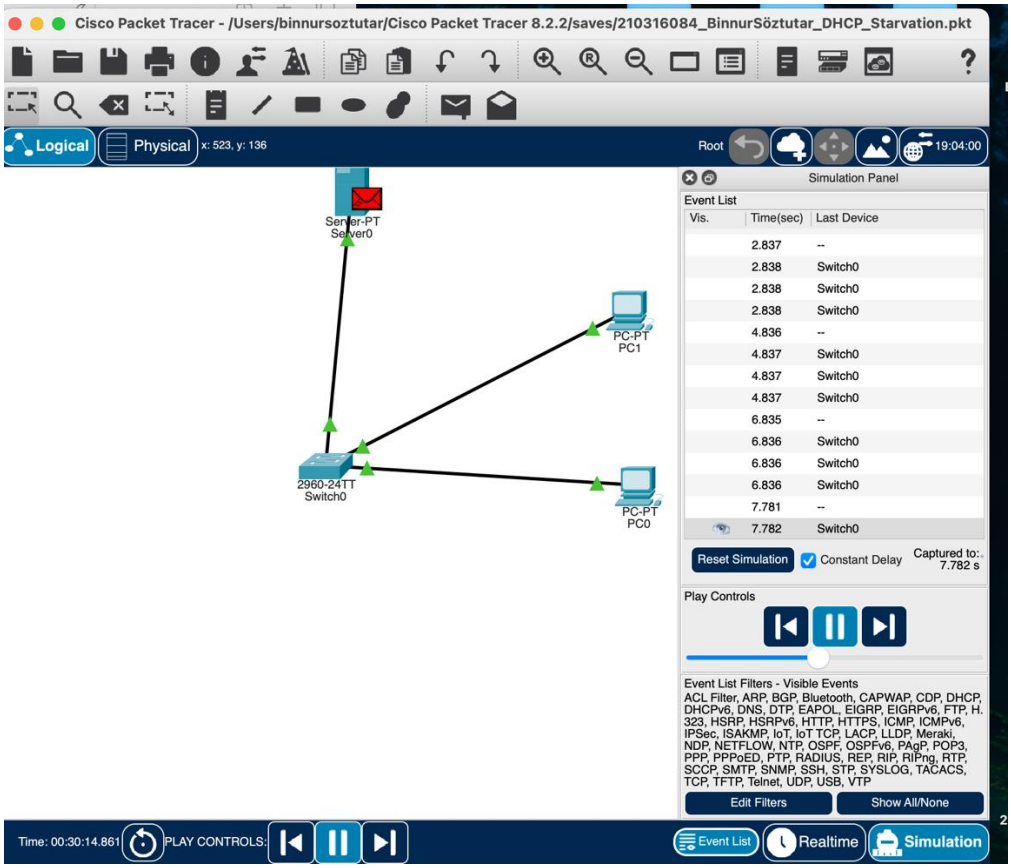
Innocent User Cannot Get IP:

Real clients, such as PC0, can no longer receive IP and are isolated from the network. APIPA IPs such as "169.x.x.x" can occur.



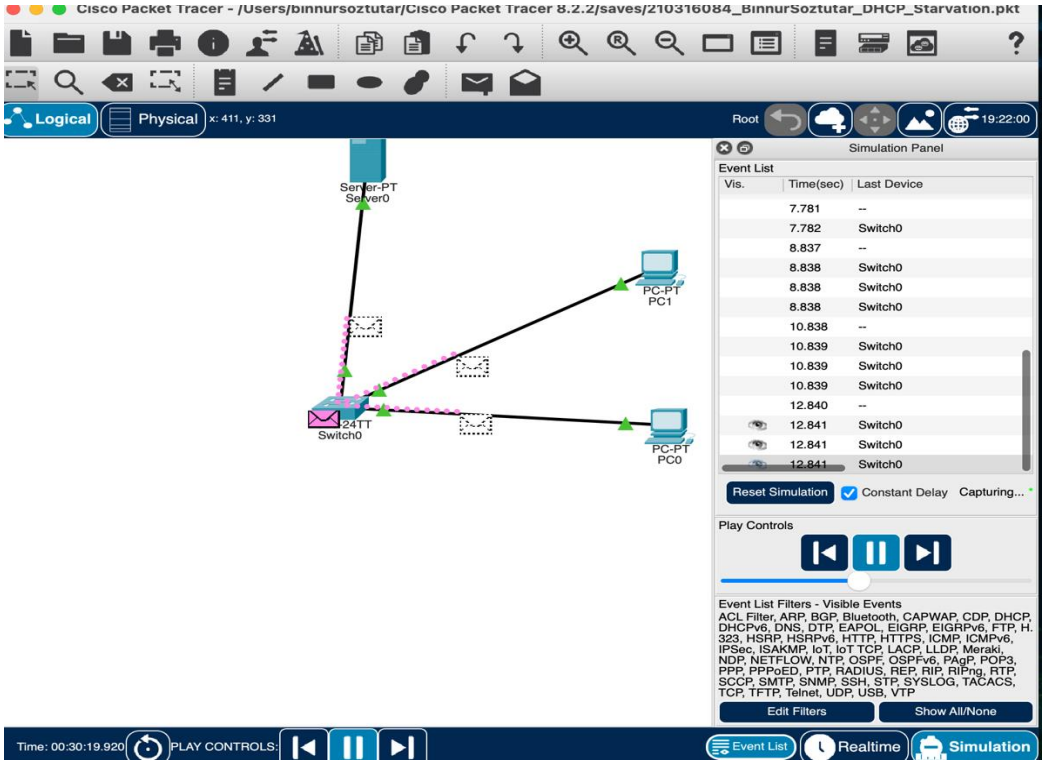
Server Under Load:

The DHCP server is having difficulty responding. The IP pool is almost exhausted.



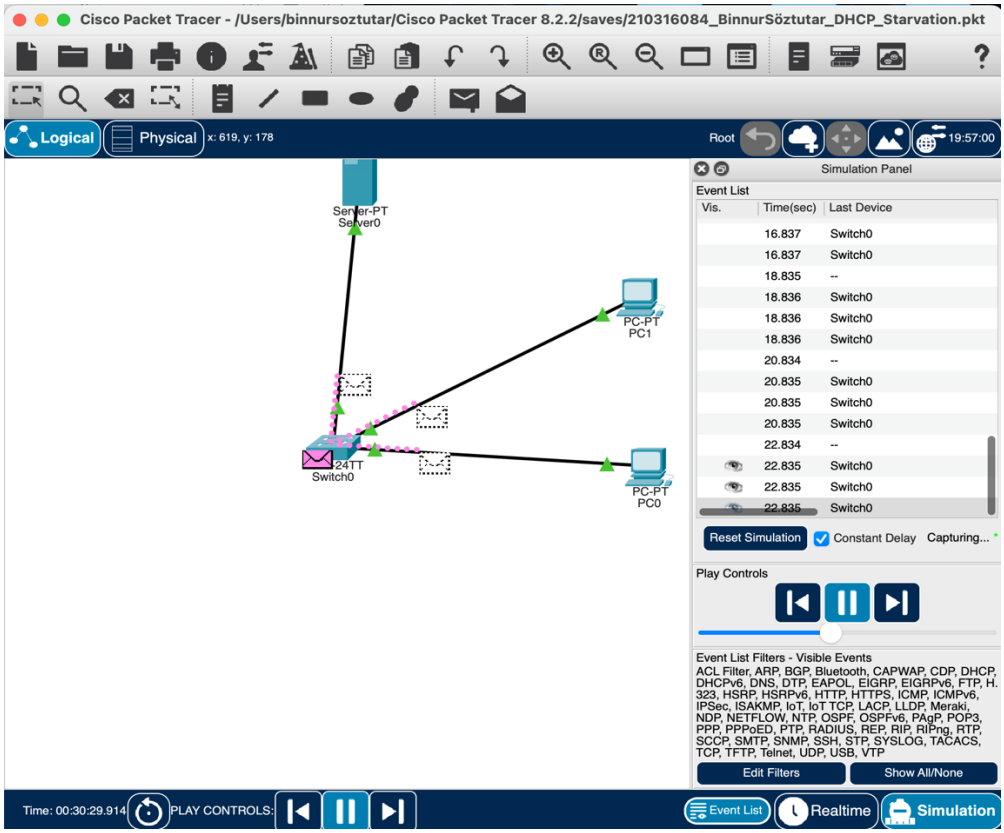
Continuously Refreshed DHCP Requests

The attacker keeps sending new requests and the attack effect increases.



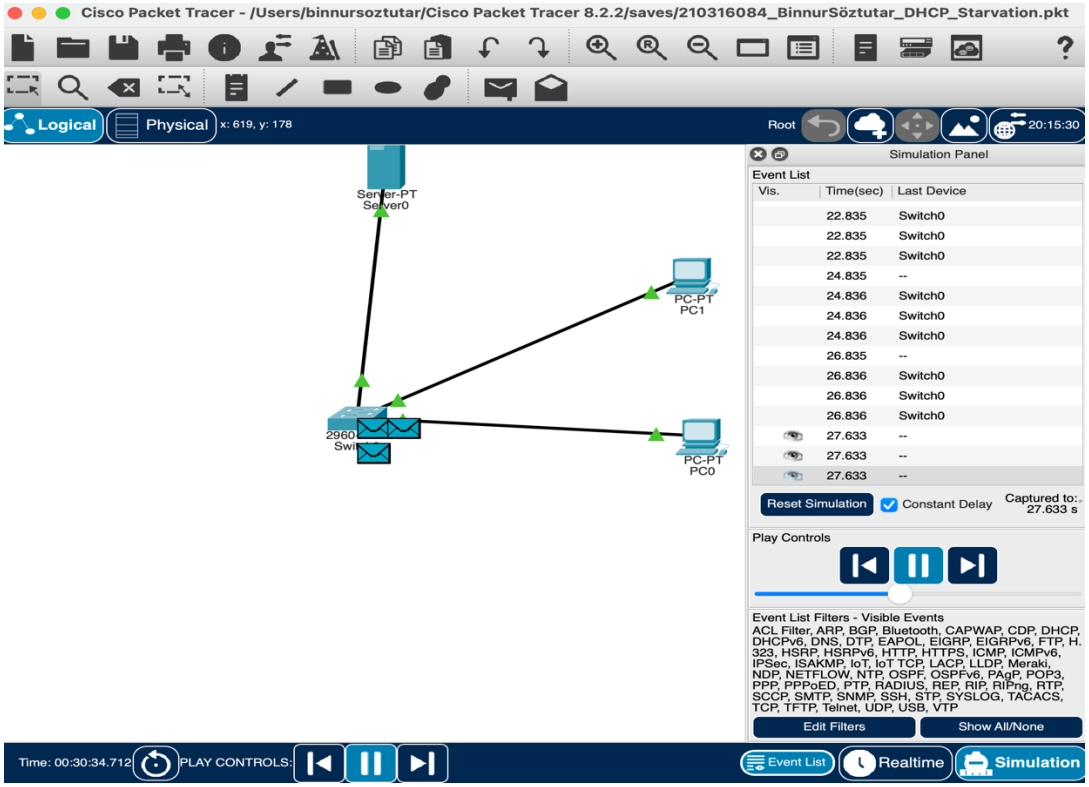
Devices that cannot connect to the network

Some devices on the network have completely stopped receiving IP. The devices can no longer communicate.



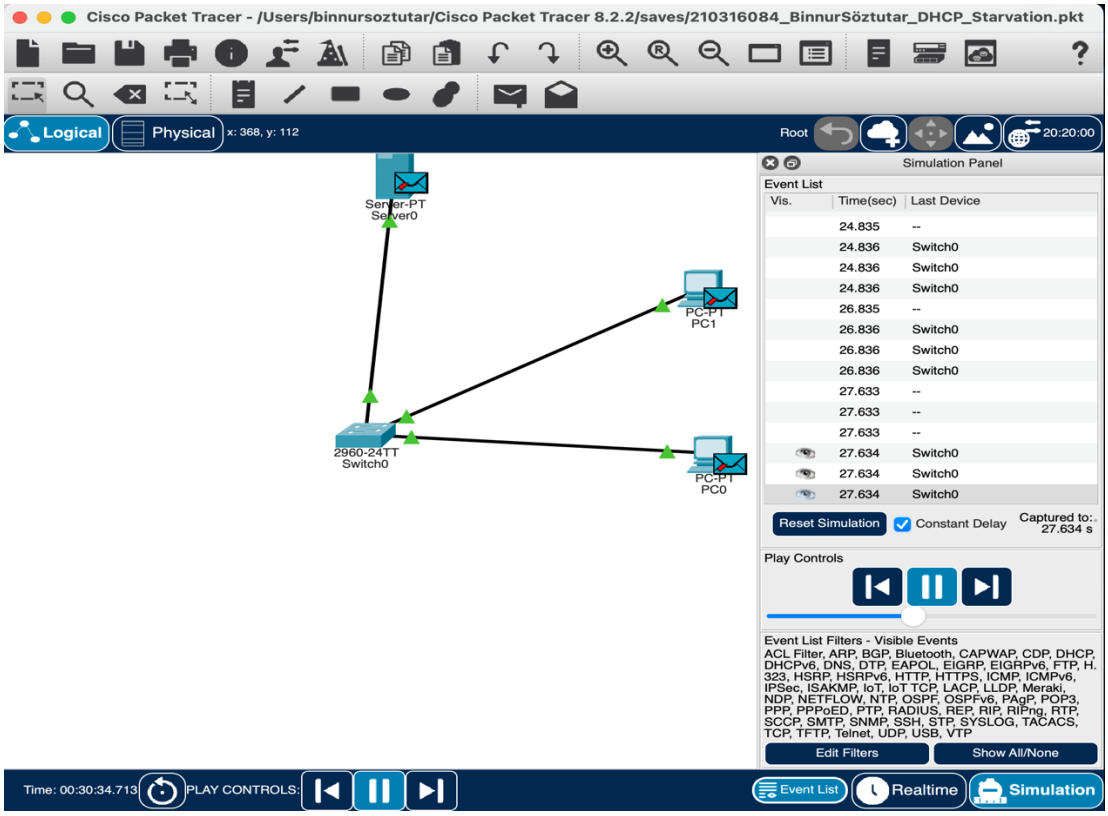
Package Loss

Some of the packets are skipped or delayed by the switch.



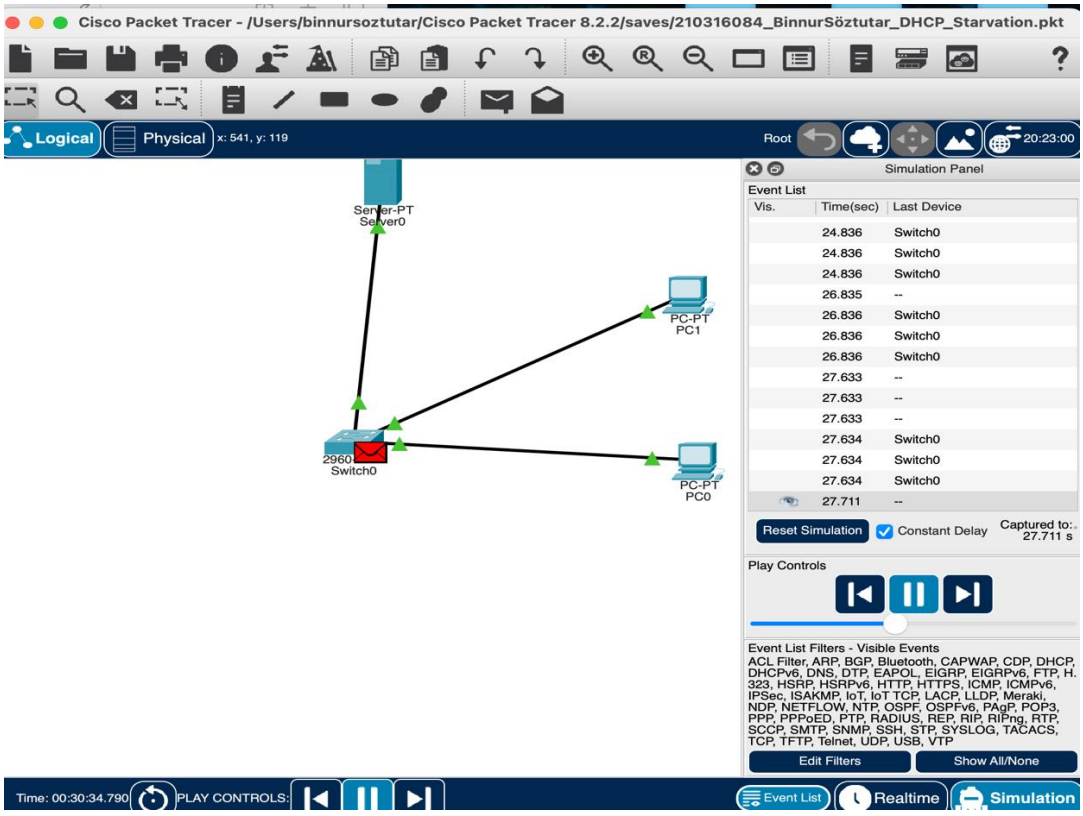
Switch Trying to Respond

Switch tries to redirect, but most requests are again unsuccessful.



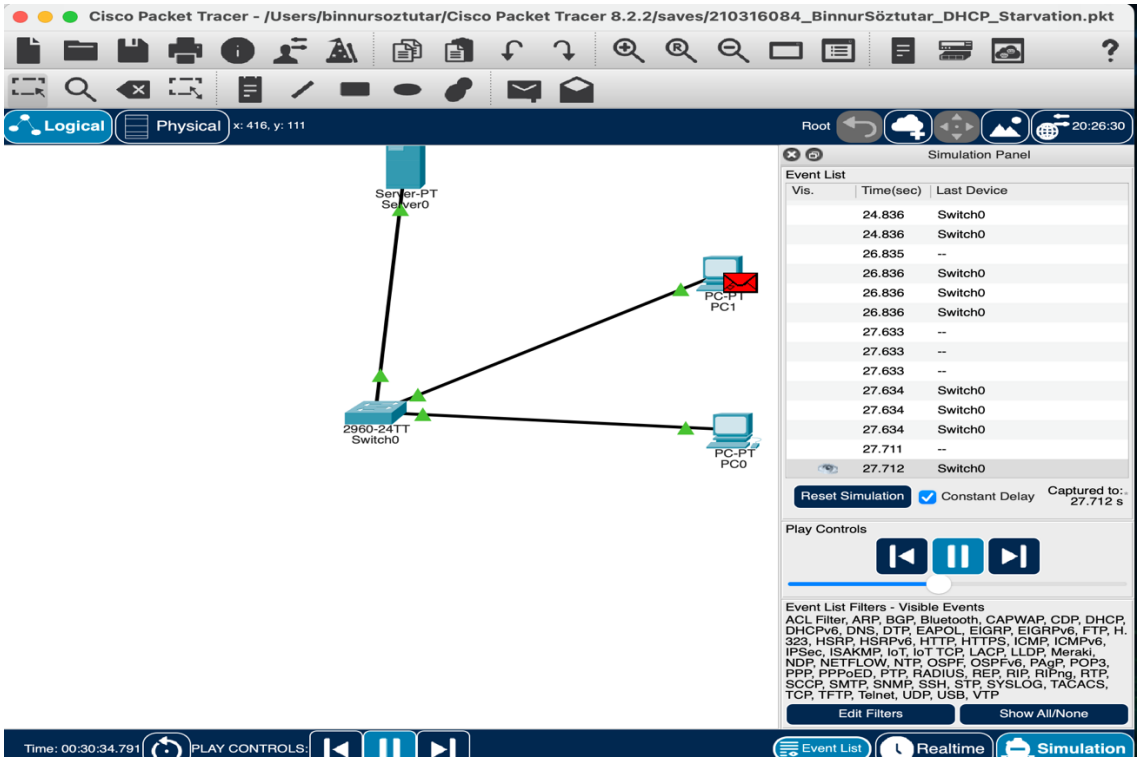
Server Completely Silent

The DHCP server can no longer respond to any clients. IP distribution has stopped.



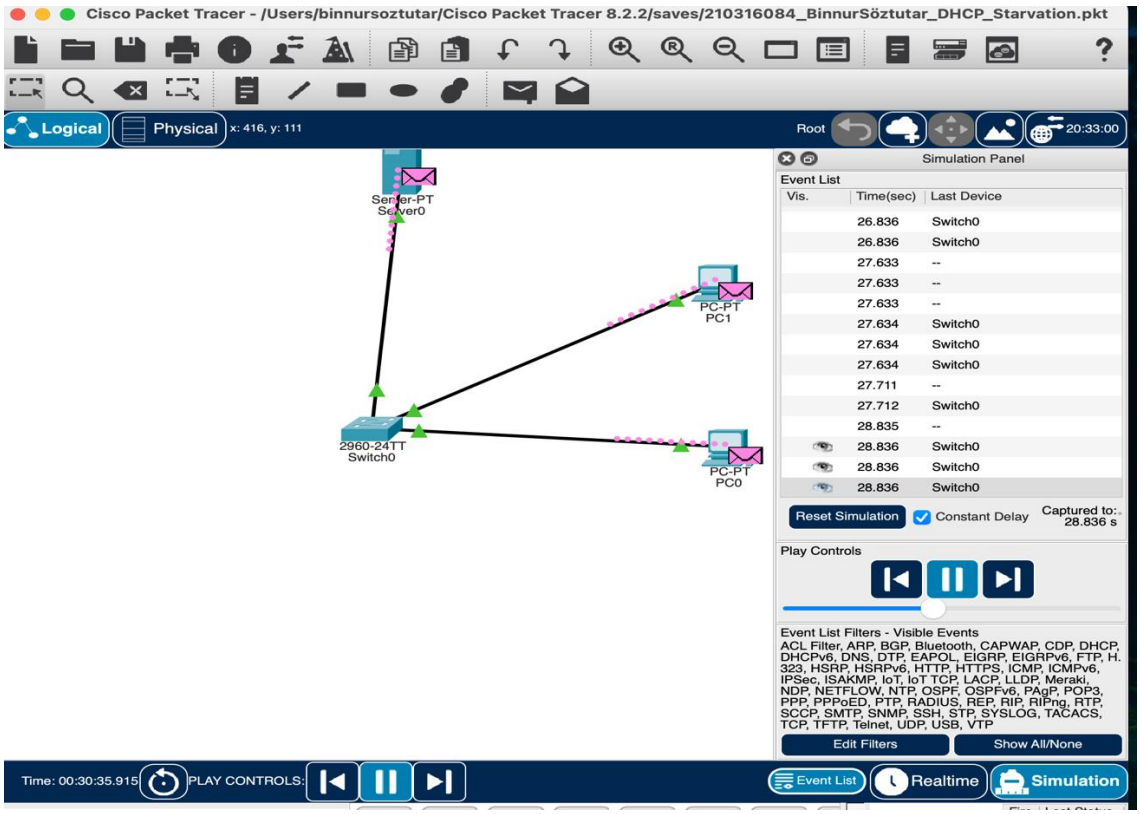
No Mobility Left in the Network

Although there is routing between devices, devices that cannot receive IP remain silent on the network.



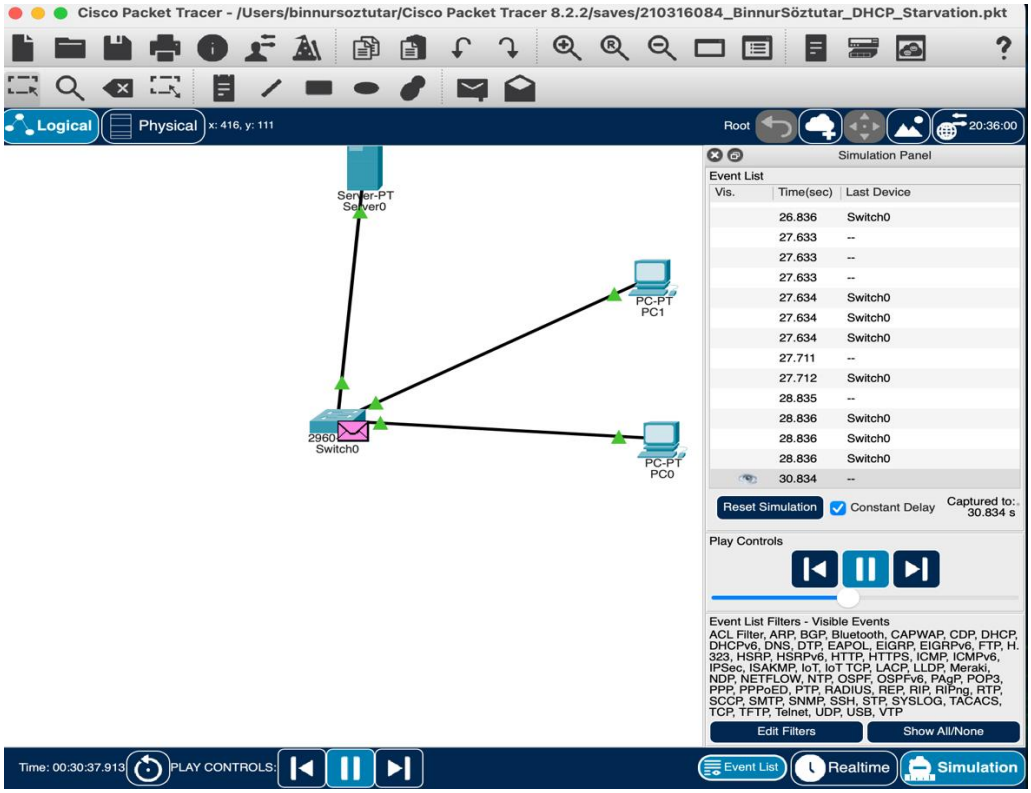
Attacker's MAC Address Appears

It is observed how systematic the attack is by changing the MAC address.



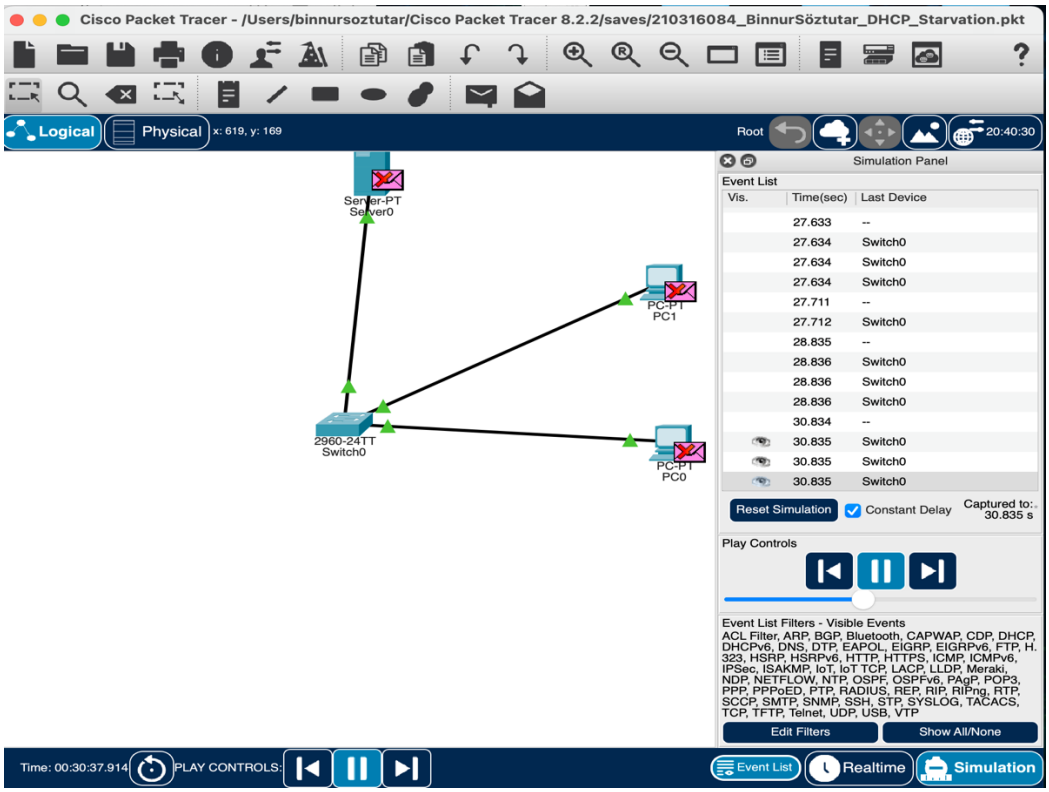
All Traffic Suspended

All DHCP packets are either suspended or lost.



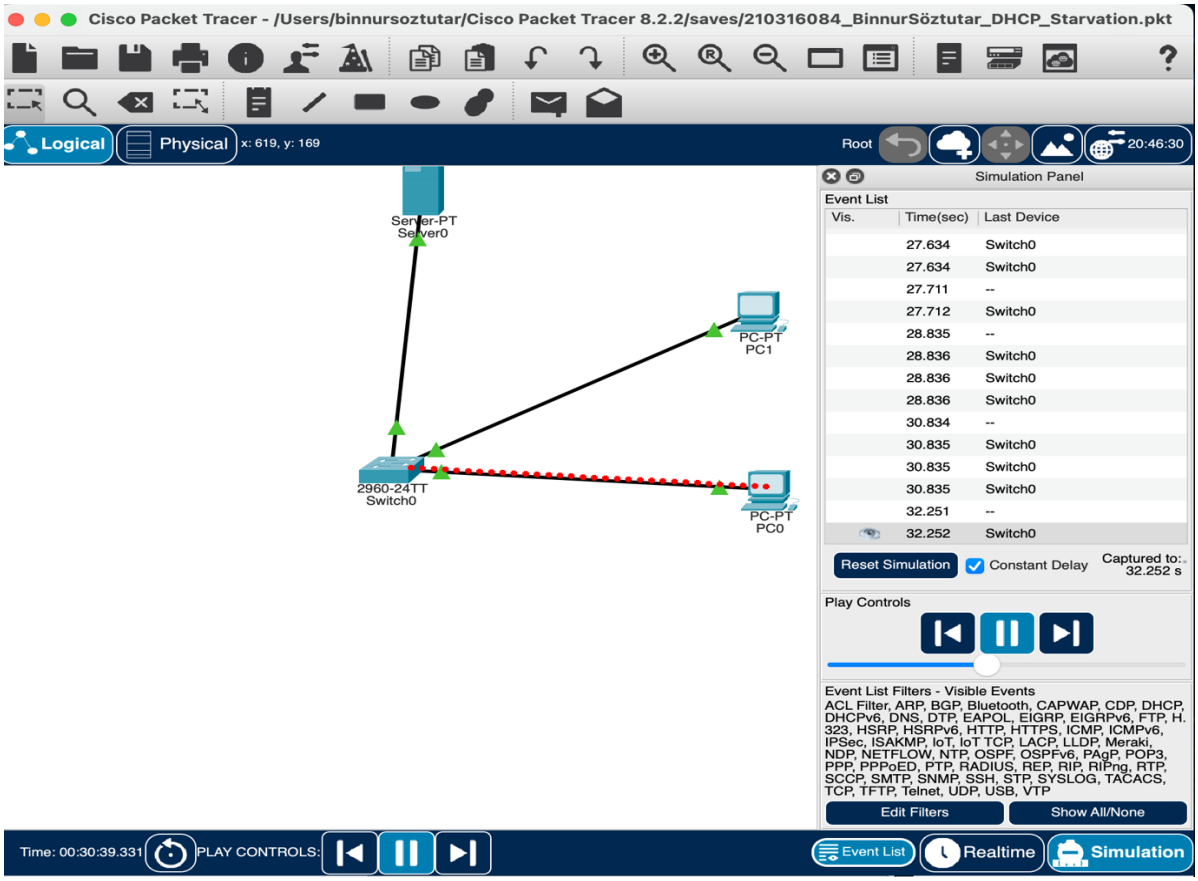
Server Responds Poorly

Server responses are slow and incomplete.



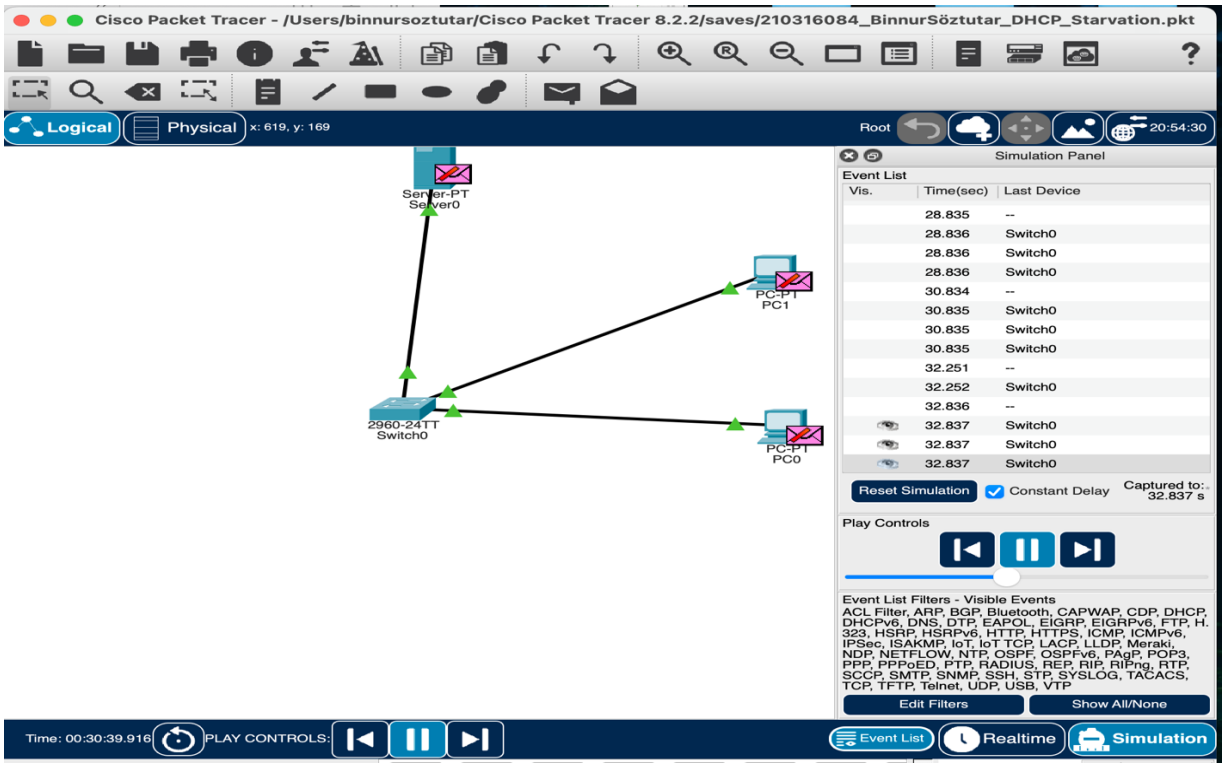
No Answer, No IP

The DHCP server no longer issues any IP, the devices in the network are ineffective.



DHCP Starvation Completed

The IP pool is completely exhausted. Real users can no longer receive IPs and connect to the network.



Technical Note:

Since attack tools such as Yersinia or DHCPig cannot be used directly in the Cisco Packet Tracer environment, this attack scenario was simulated with manual MAC address changes. In order to create fake clients, the MAC address of the attacking device was changed each time and new requests were sent to the DHCP server. This method was chosen to visually represent the effects of a real DHCP Starvation attack.

Simulation Environment and File Information

The DHCP Starvation attack scenario created within the scope of this project was manually configured in the Cisco Packet Tracer environment. Since real attack software (e.g. Yersinia, DHCPig) cannot be run directly in Cisco Packet Tracer, the attack scenario was simulated with fake MAC address changes. The goal is to present the effects of the attack functionally and visually.

Simulation file name:

P1_210316084_BinnurSöztutar_DHCP_Starvation_Problem.pkt

CONCLUSION:

As a result of the DHCP Starvation attack in this scenario, the IP distribution on the network was completely blocked, and the DHCP server and switch were unable to continue their normal functions. Real users could not connect to the network because they could not get an IP address, and network services were completely disabled. This situation reveals how critical the attacks made by exploiting the weak points of the DHCP protocol can have critical consequences.