Static IP - DHCP IP Conflict Problem

Static IP - DHCP IP conflict is a network problem that occurs when the same IP address is both automatically assigned by the DHCP server and manually (statically) configured on another device. This causes an IP addressing conflict at the Layer 3 (Network Layer) level.

The main causes of this error:

-The statically assigned IP address is outside the control of the DHCP server. When DHCP distributes an IP, it does not check whether that address is on another device. Therefore, the same IP can be assigned to two different devices.

-DHCP pool coverage may be misconfigured.

-An address from the pool may have been selected when assigning a static IP.

-Users who are not network administrators may have performed the manual IP assignment incorrectly.

As a result of this overlap:

-Two different devices try to use the same IP address at the same time on the network.

Different MAC addresses can be seen against the same IP in the -ARP (Address Resolution Protocol) table.

-Error messages such as "Duplicate IP Detected" or "IP Address Conflict" are received on the network.

-DHCP or network routing is unstable, disconnections occur.

OSI Layer Layer 3

Symptoms of Detection

An IP conflict warning appears on the network.

Even if the devices ping, data loss occurs.

One device loses the connection or both are out of the network.

Different MAC addresses appear in the ARP table to the same IP.

Broadcast increase can be observed on Switch.

Admin Guide - Remedy and Prevention Steps

Such conflicts require careful configuration both to protect the existing network and to prevent future outages. The following steps are an implementation and audit guide for network administrators:

Step 1: Define DHCP Pool Correctly

When determining the IP pool on the DHCP server, an out-of-range static IP region should be reserved for devices to be given manual IP.

Example:

DHCP Pool: 192.168.1.100 - 192.168.1.200

Static IPs: 192.168.1.2 - 192.168.1.50

Step 2: Document Static IP Assignments

All devices assigned a static IP (for example: printer, IP camera, server) should be recorded in an inventory table. Make sure that these IPs are outside the DHCP pool.

Step 3: Track IP Conflicts

Switch and router logs should be monitored and messages such as "Duplicate IP detected" should be analysed. If necessary, the ARP table should be examined and different MAC addresses belonging to the same IP should be checked:

PC> arp -a

Step 4: Using DHCP Reservation

If a device-specific static IP is to be defined, it is safer to make a reservation by MAC address on the DHCP server, so that a specific IP is assigned only to a specific device, preventing IP conflicts.

Step 5: Access Restriction

Only network administrators should be allowed to make such configurations with access restrictions.

Simulation Visuals and Descriptions: IP Conflict (Static IP-DHCP Conflict)

1 DHCP server (Server0)

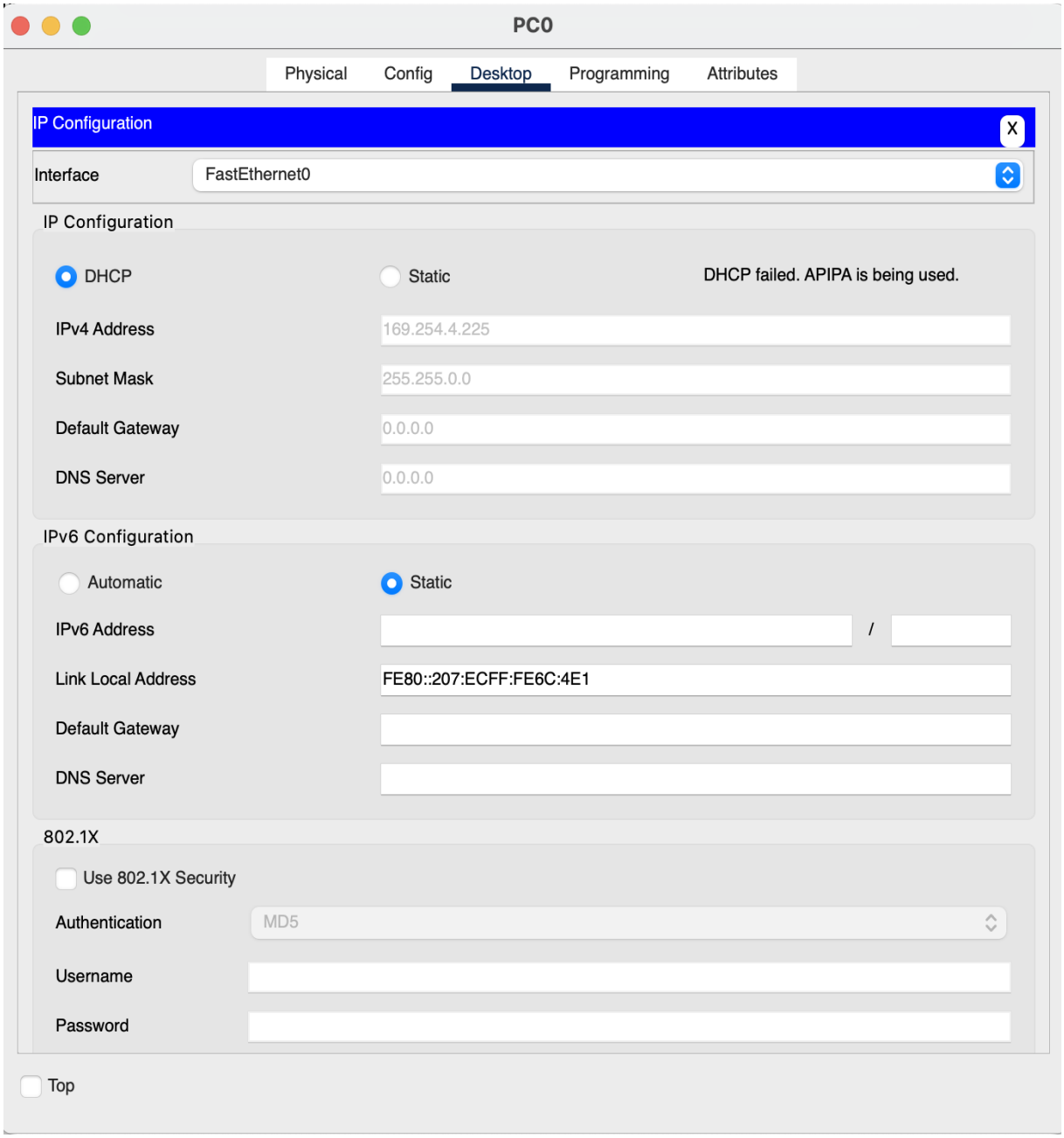
2 computers (PC0 and PC1)

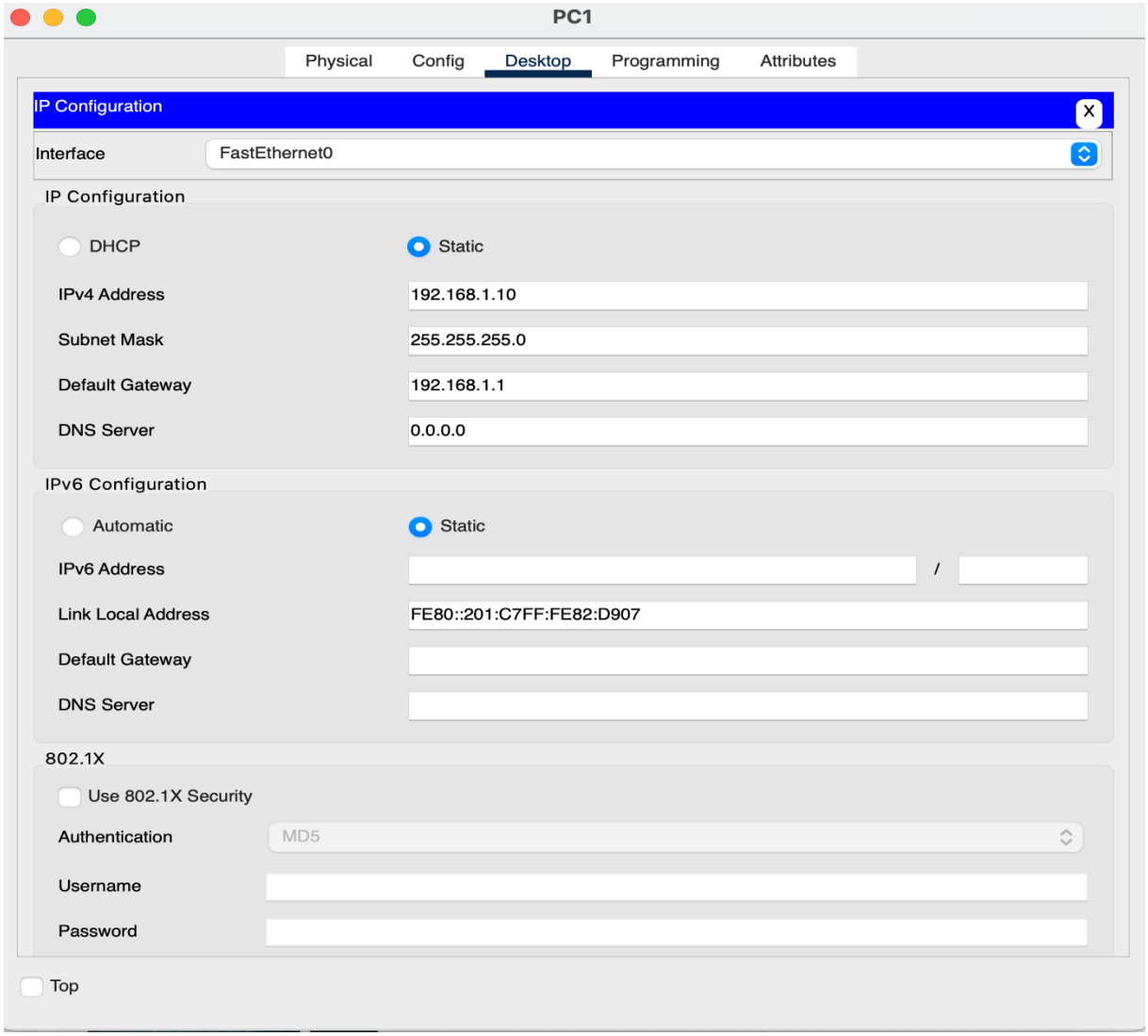
1 switch (Switch0)

IP addressing:

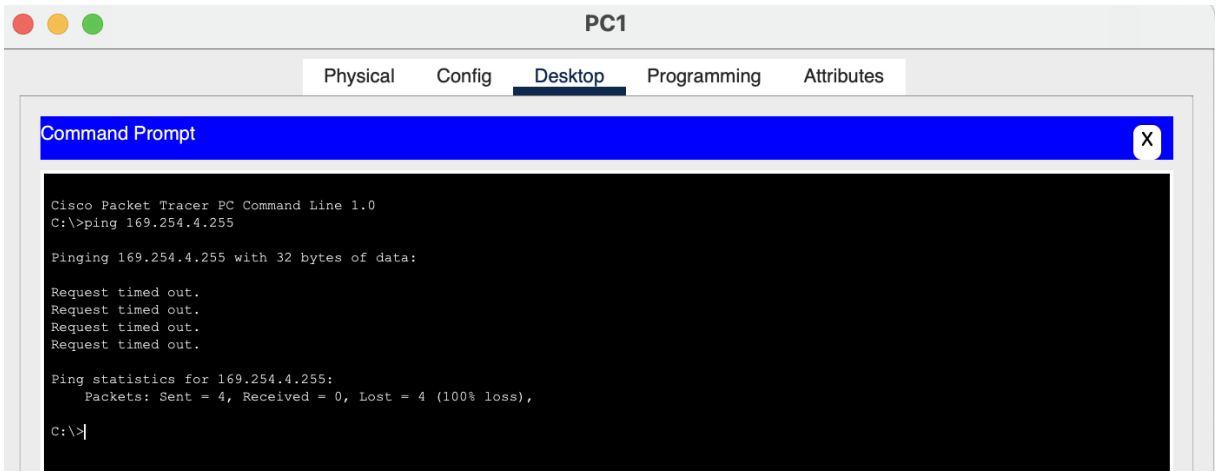
PC0: Set to receive automatic IP from DHCP.

PC1: 192.168.1.10 is assigned as static IP.

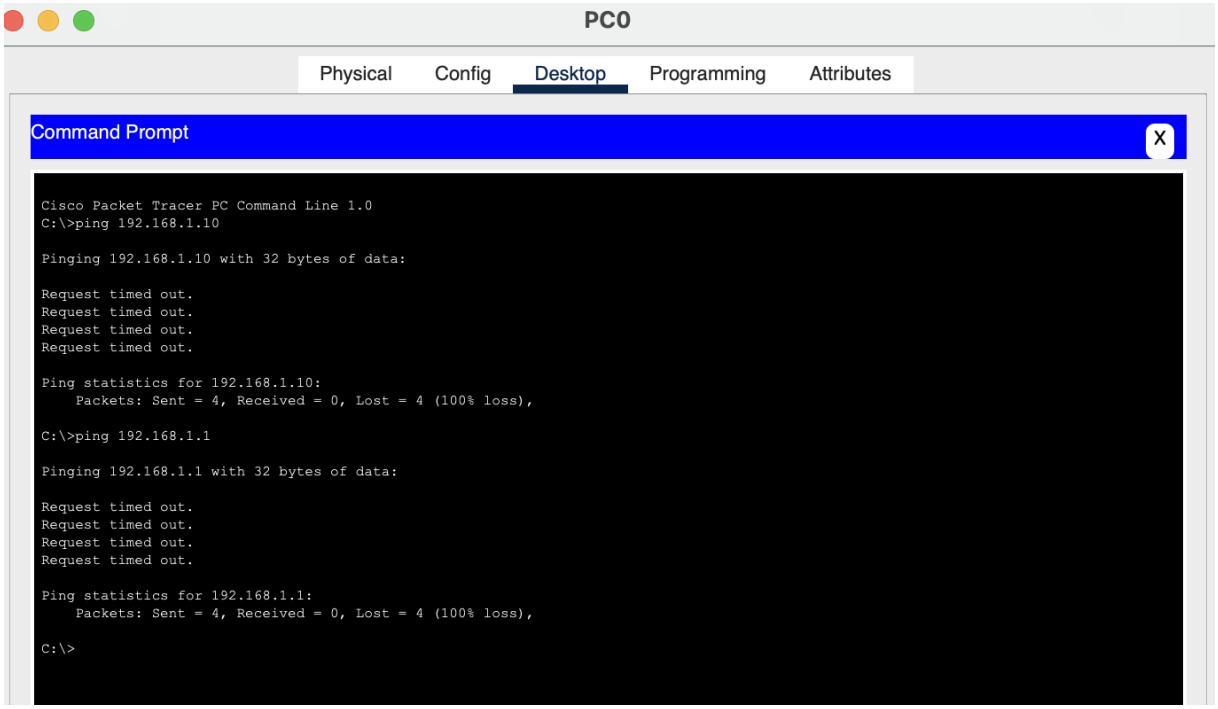




Ping Tests:



PC1 could not get a healthy IP from DHCP due to IP conflict and automatically received an address from the **169.254.x.x** block via **APIPA** (Automatic Private IP Addressing). Since these addresses are non-routable, it is normal to fail the ping test.



PC0 failed to ping both the static assigned IP (192.168.1.10) and the gateway (192.168.1.1). This indicates that the IP conflict is affecting all communication on the network and routing is not available.

Simulation Outputs:

During the simulation, a network environment was created with two computers (PC0 and PC1) and a DHCP server connected. The DHCP service configured on Server0 is defined to distribute the range 192.168.1.10-192.168.1.19 as an IP pool. Meanwhile, PC1 is statically assigned an IP address (192.168.1.10) in the same range.

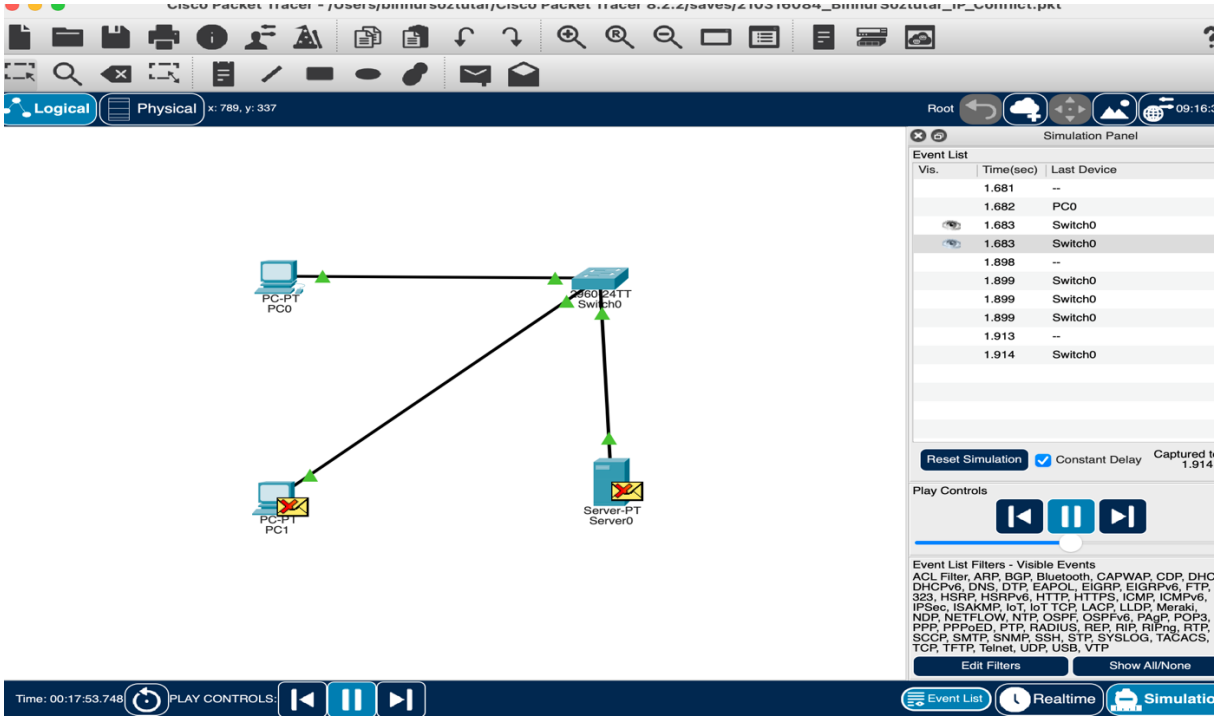
Simulation flow:

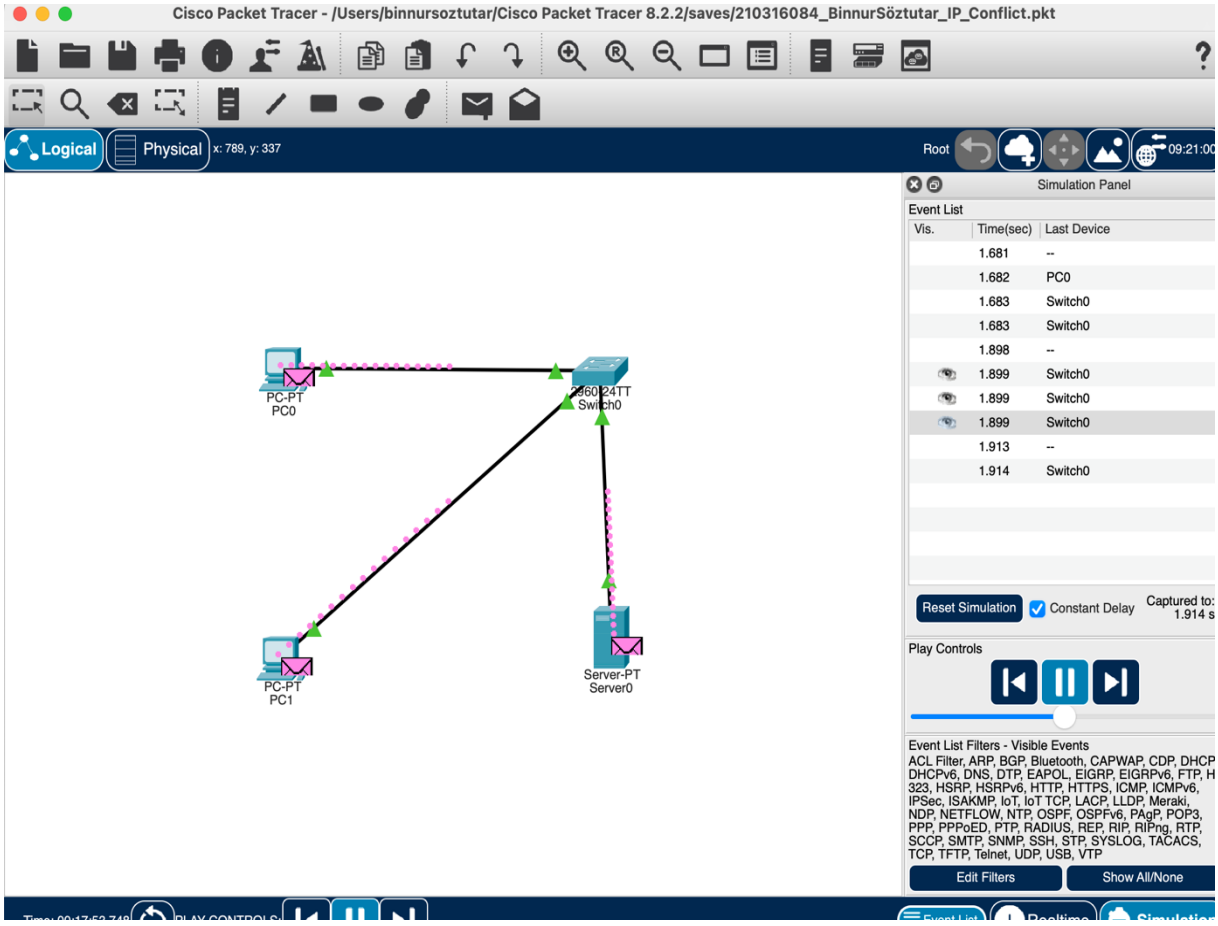
PC0, trying to get an IP via DHCP, could not get an address from the DHCP server due to an IP conflict and automatically received a temporary address from the APIPA (169.254.x.x) block.

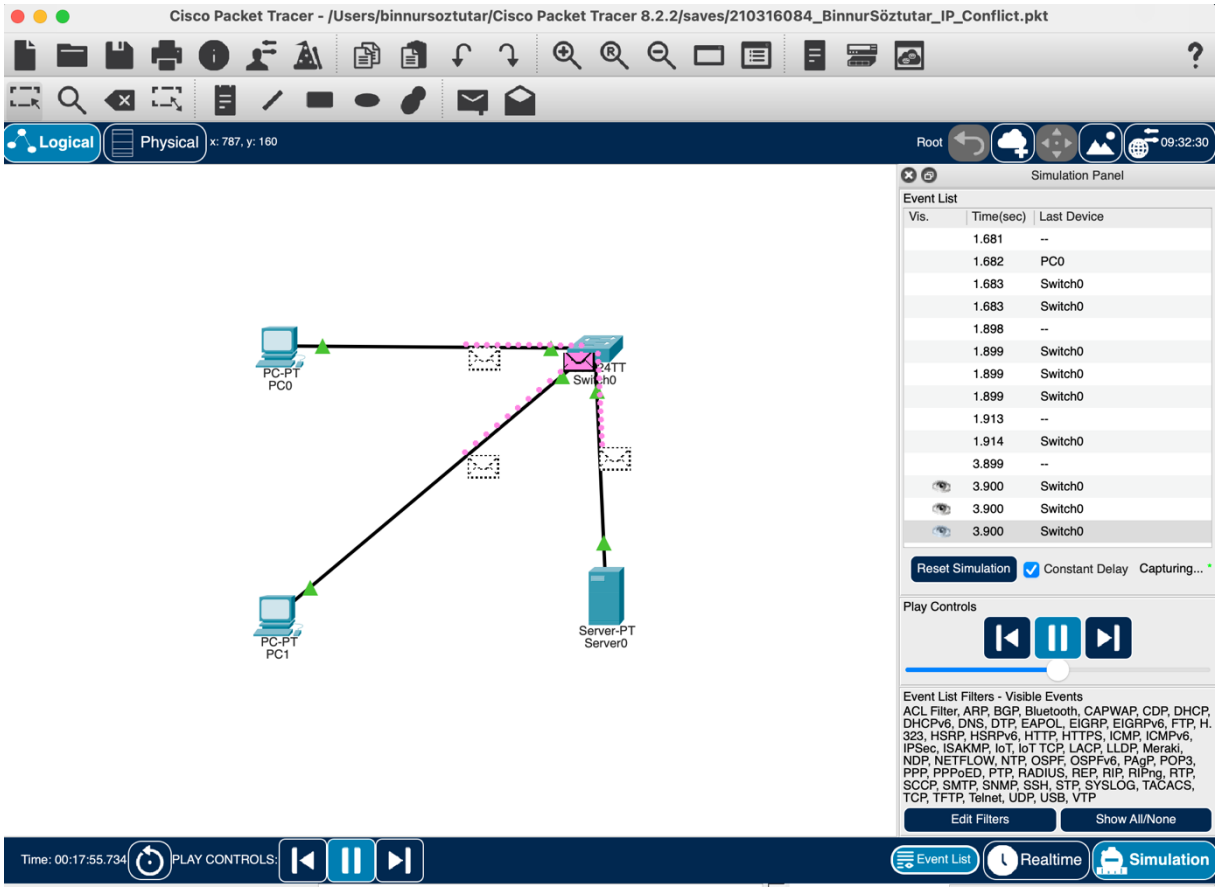
PC1, which was configured with static IP at the same time, could not communicate because it was already using the IP used by another device on the network.

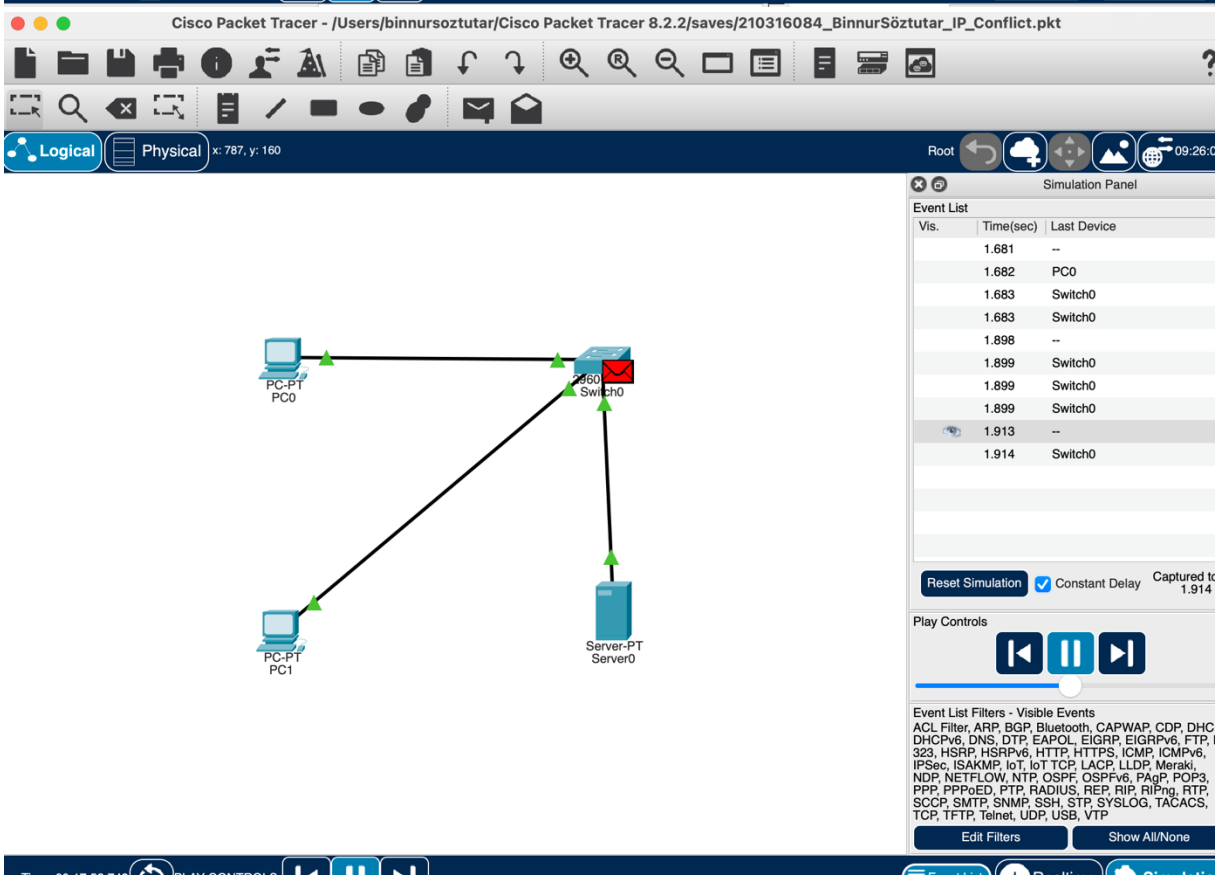
Red X marks and transmission errors were observed on the switch connections. This indicates that correct routing could not be done due to collision and data packets could not reach their destination.

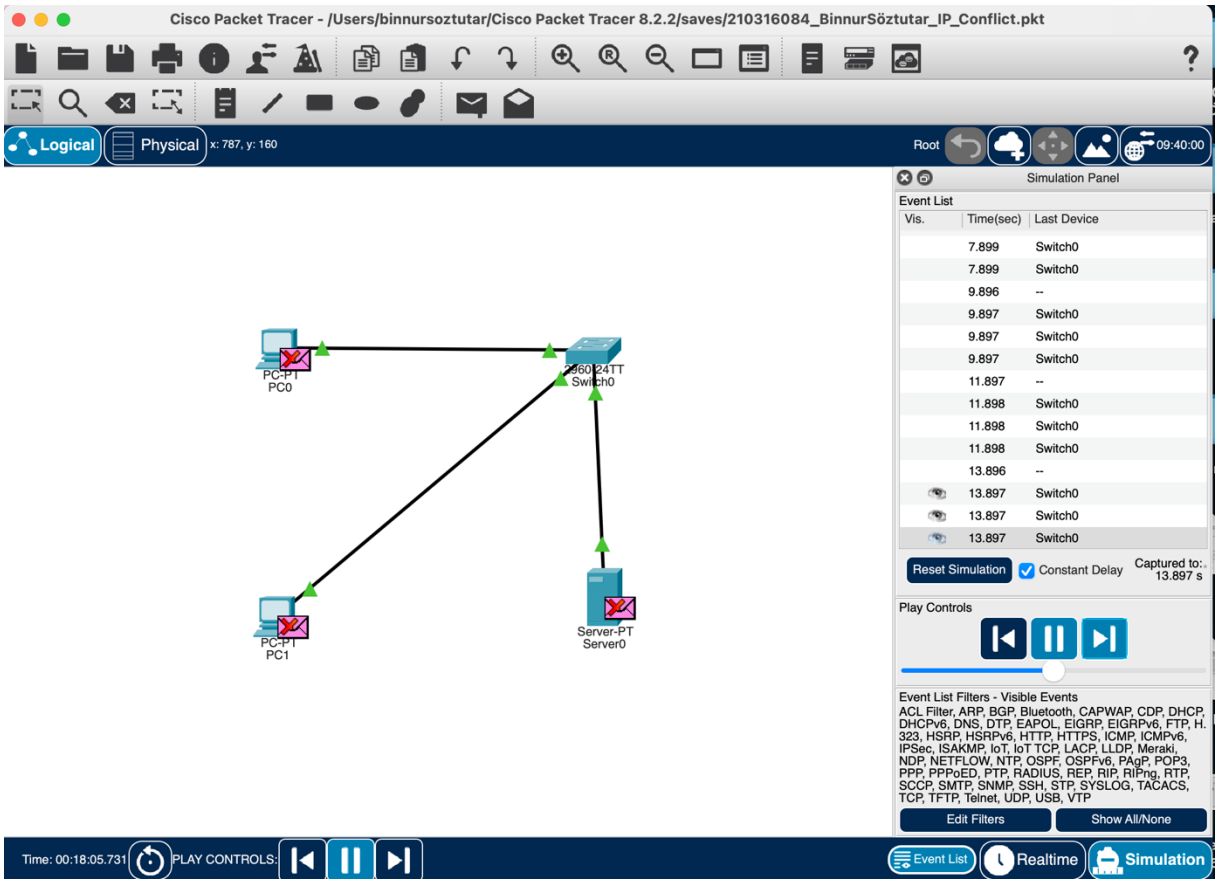
Ping tests failed. All ping requests gave a "Request timed out" error. This proves that communication between devices is not possible due to IP conflicts on the network. This scenario clearly demonstrates how the collision of IPs in the DHCP pool with random static assignment renders the entire network ineffective and why network administrators need to perform careful IP planning.


Logical
Physical
x: 789, y: 337
Root
Simulation Panel
Event List
Vis. Time(sec) Last Device
1.681 --
1.682 PC0
1.683 Switch0
1.683 Switch0
1.898 --
1.899 Switch0
1.899 Switch0
1.899 Switch0
1.913 --
1.914 Switch0
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
PC-PT PC0
2960-24TT Switch0
PC-PT PC1
Server-PT Server0
Time: 00:17:53.748
PLAY CONTROLS:
Event List
Realtime


Cisco Packet Tracer - /Users/binnursoztutar/Cisco Packet Tracer 8.2.2/saves/210316084_BinnurSöztutar_IP_Conflict.pkt
Logical
Physical
x: 789, y: 337
Root
Simulation Panel
Event List
Vis. Time(sec) Last Device
1.681 --
1.682 PC0
1.683 Switch0
1.683 Switch0
1.898 --
1.899 Switch0
1.899 Switch0
1.899 Switch0
1.913 --
1.914 Switch0
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
PC-PT PC0
2960-24TT Switch0
PC-PT PC1
Server-PT Server0


Cisco Packet Tracer - /Users/binnursoztutar/Cisco Packet Tracer 8.2.2/saves/210316084_BinnurSöztutar_IP_Conflict.pkt
Logical
Physical
x: 787, y: 160
Root
09:32:30
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
1.681 --
1.682 PC0
1.683 Switch0
1.683 Switch0
1.898 --
1.899 Switch0
1.899 Switch0
1.899 Switch0
1.913 --
1.914 Switch0
3.899 --
3.900 Switch0
3.900 Switch0
3.900 Switch0
Reset Simulation
Constant Delay
Capturing...
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:17:55.734
PLAY CONTROLS:
Event List
Realtime
Simulation
PC-PT PC0
PC-PT PC1
Server-PT Server0


Cisco Packet Tracer - /Users/binnursoztutar/Cisco Packet Tracer 8.2.2/saves/210316084_BinnurSöztutar_IP_Conflict.pkt
Logical
Physical
x: 787, y: 160
Root
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
1.681 --
1.682 PC0
1.683 Switch0
1.683 Switch0
1.898 --
1.899 Switch0
1.899 Switch0
1.899 Switch0
1.913 --
1.914 Switch0
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
PC-PT PC0
PC-PT PC1
Server-PT Server0



Simulation File name:
P4_210316084_BinnurSöztutar_IP_Conflict.pkt