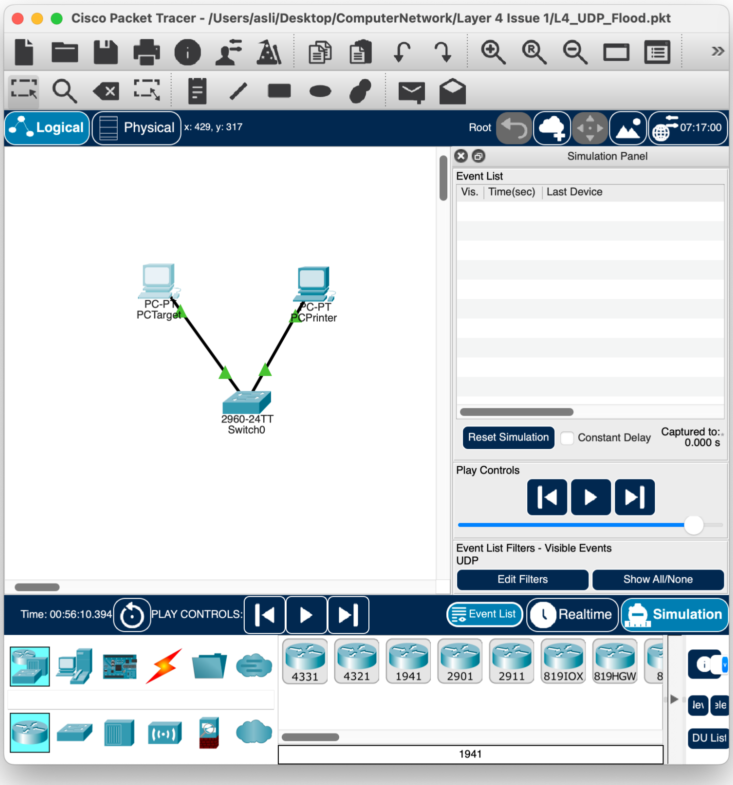
L4 – UDP Flood Attack Against Shared Dormitory Printer Explanation

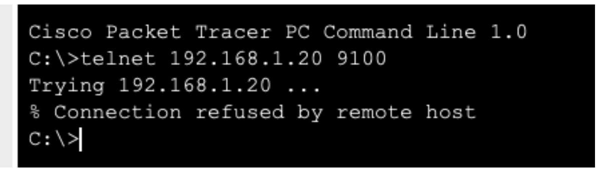
Printers typically listen on several UDP ports:
Port 9100 – for raw printing
Port 161 – SNMP communication
The continuous stream of random UDP packets overwhelmed the printer's network interface, leading to a denial-of-service (DoS) condition where the printer could no longer process valid traffic.



Cisco Packet Tracer - /Users/asli/Desktop/ComputerNetwork/Layer 4 Issue 1/L4_UDP_Flood.pkt

Event List Filters - Visible Events
UDP

Attack Simulation:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.20 9100
Trying 192.168.1.20 ...
% Connection refused by remote host
C:\>
```

Simulation Mode:
Enabled **UDP-only** filters
Observed packet flow from PC0 to PC1
Printer (PC1) responded with figure above.

This is a classic Layer 4 (Transport Layer) vulnerability exploiting UDP's connectionless design. Without session validation or throttling, devices listening on open ports are susceptible to overloads.