**Ex No: 9**

**Date:**

**ANALYZE THE NETWORK TRAFFIC USING PACKET TRACER TOOL.**

**Aim:**

To simulate a simple LAN connection with server and four end users, implement any one of the TCP applications(HTTP, DNS etc), generate and analyze the network traffic, for each step of transmission in simulation.

**Theory:**

**Network Traffic Analysis** refers to the process of capturing, inspecting, and interpreting network packets transmitted over a network. This helps in understanding the behavior of applications, identifying potential security issues, and optimizing network performance.

* **Purpose**:
  + Monitoring network health and performance.
  + Detecting security threats such as intrusions or malware.
  + Debugging network-related issues.
  + Ensuring compliance with network policies.
* **Key Metrics**:
  + **Packet Size**: The amount of data in each packet.
  + **Protocol Used**: Common protocols like TCP, UDP, HTTP, or DNS.
  + **Source and Destination IP**: Identifying the endpoints of communication.
  + **Throughput and Latency**: Measuring data transmission rates and delays.
  + **Error Rates**: Identifying corrupted or dropped packets.

**Procedure:**

**Setup the Network Simulation Environment**:

* Use a simulation tool like Cisco Packet Tracer, GNS3, or NS2.
* Create a network topology with:
  + One server (configured to host the TCP application).
  + Four client nodes (end users).
  + A switch/router to connect the nodes.

**Configure the Network**:

* Assign IP addresses to all devices within the same subnet.
* Ensure proper connectivity between devices using ping tests.

**Deploy the TCP Application**:

* For HTTP:
  + Set up a web server on the server machine.
  + Configure client devices to request web pages via a browser or a script.
* For DNS:
  + Set up a DNS server (e.g., BIND).
  + Configure clients to send DNS queries for domain name resolution.

**Simulate Network Traffic**:

* Initiate requests from each client to the server.
* Capture the traffic generated using the built-in tools in the simulator or external packet analyzers like Wireshark.

**Capture and Analyze Traffic**:

* Identify the sequence of packets exchanged (SYN, ACK, DATA).
* Observe metrics like:
  + Packet sizes and transmission intervals.
  + Source and destination IPs.
  + Protocol details and response times.

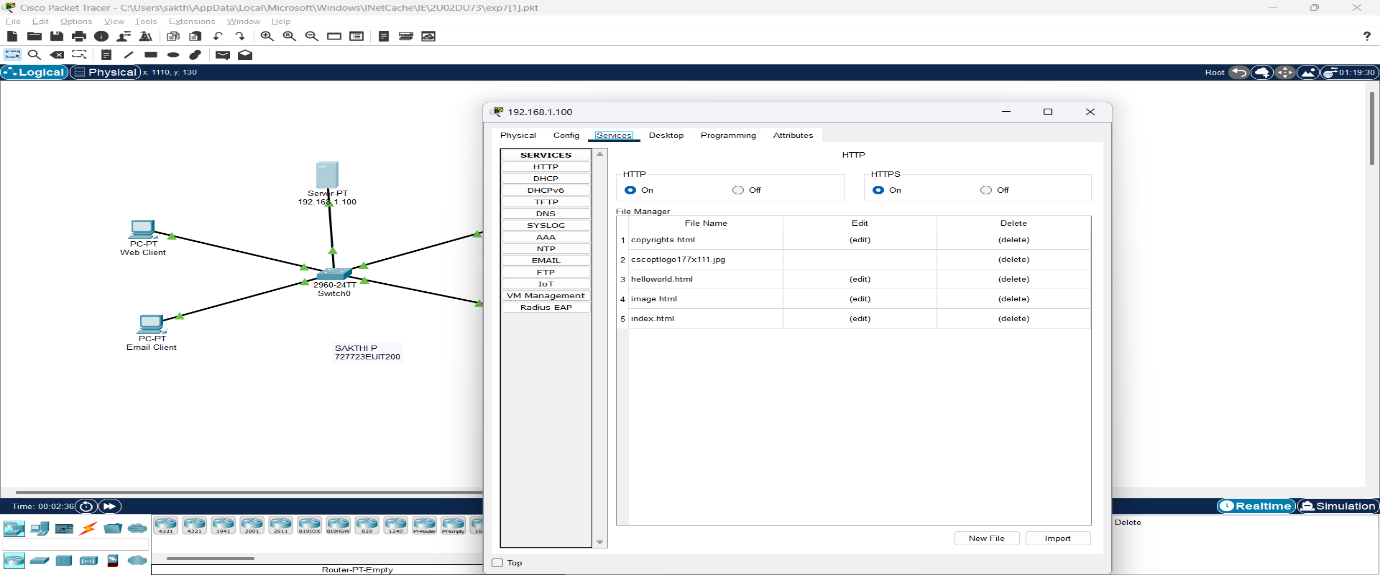
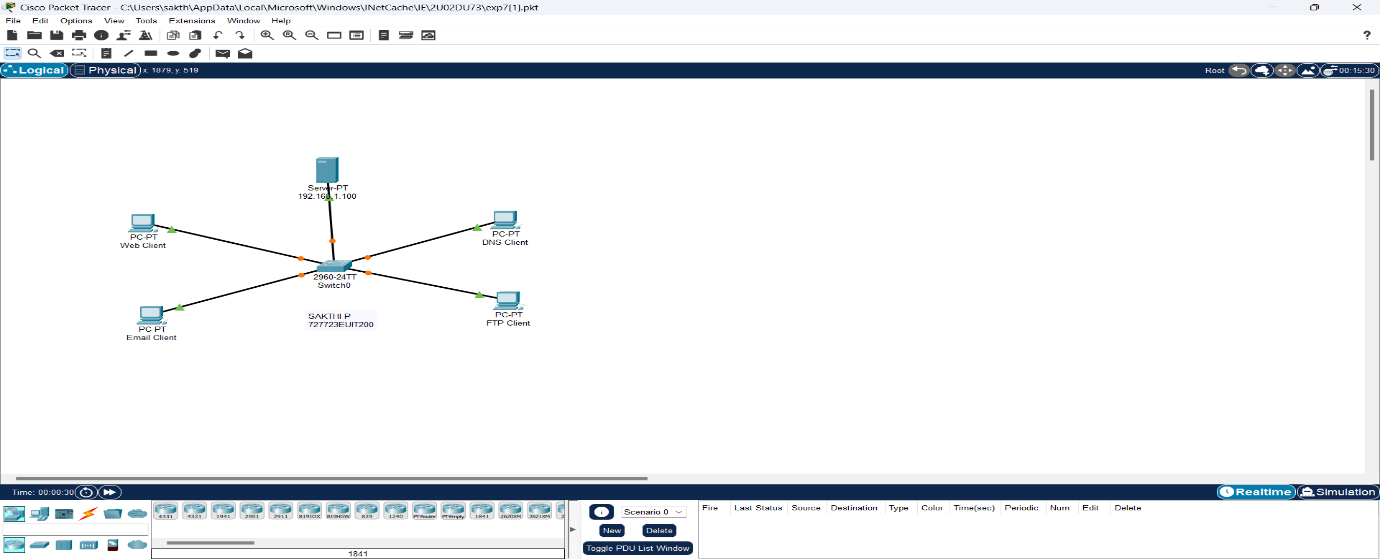
**Analyze the Results**:

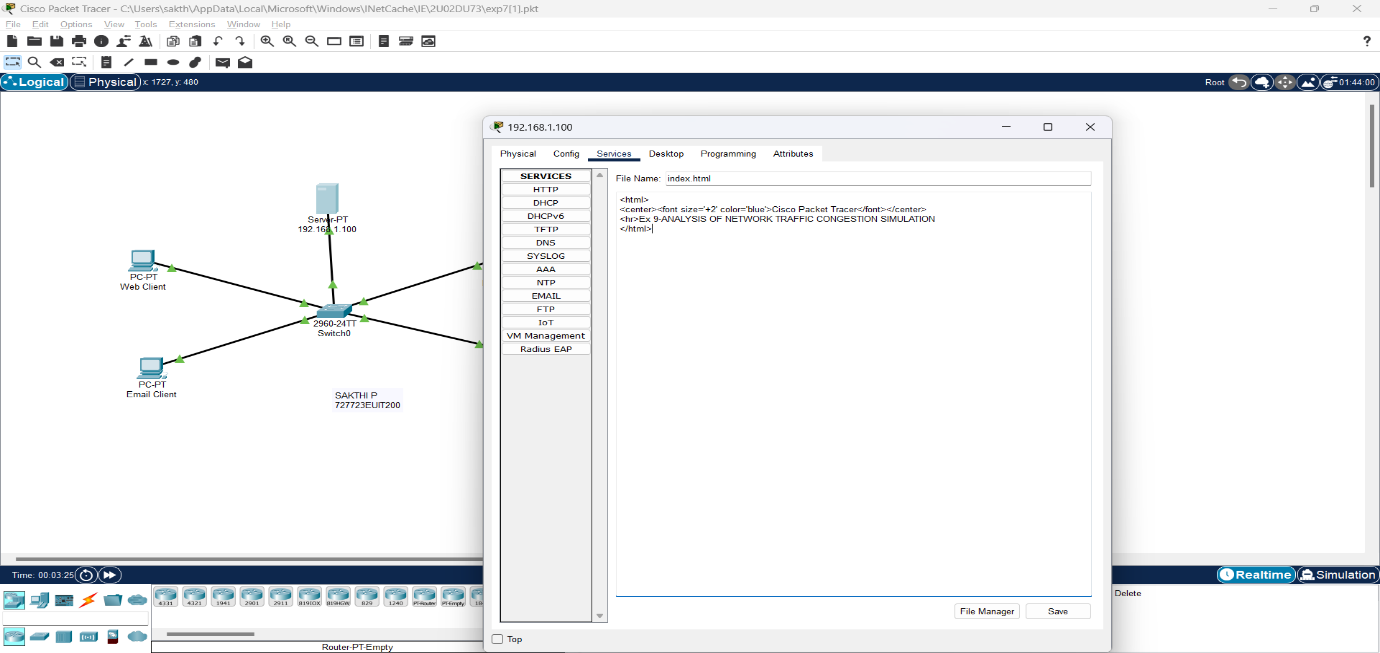
* Visualize traffic patterns in a graph (e.g., throughput over time).
* Identify anomalies or inefficiencies.
* Compare the performance under varying loads (e.g., one user vs. all four users).

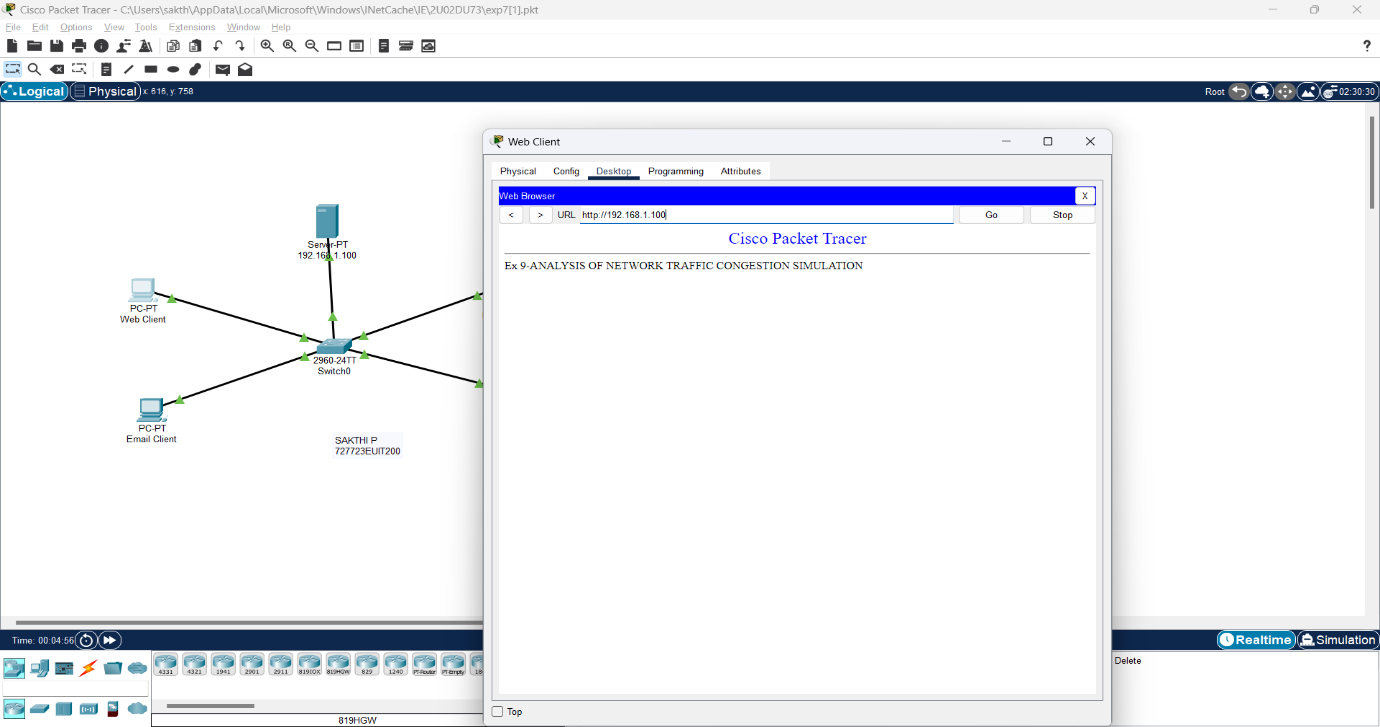
**Document Observations**:

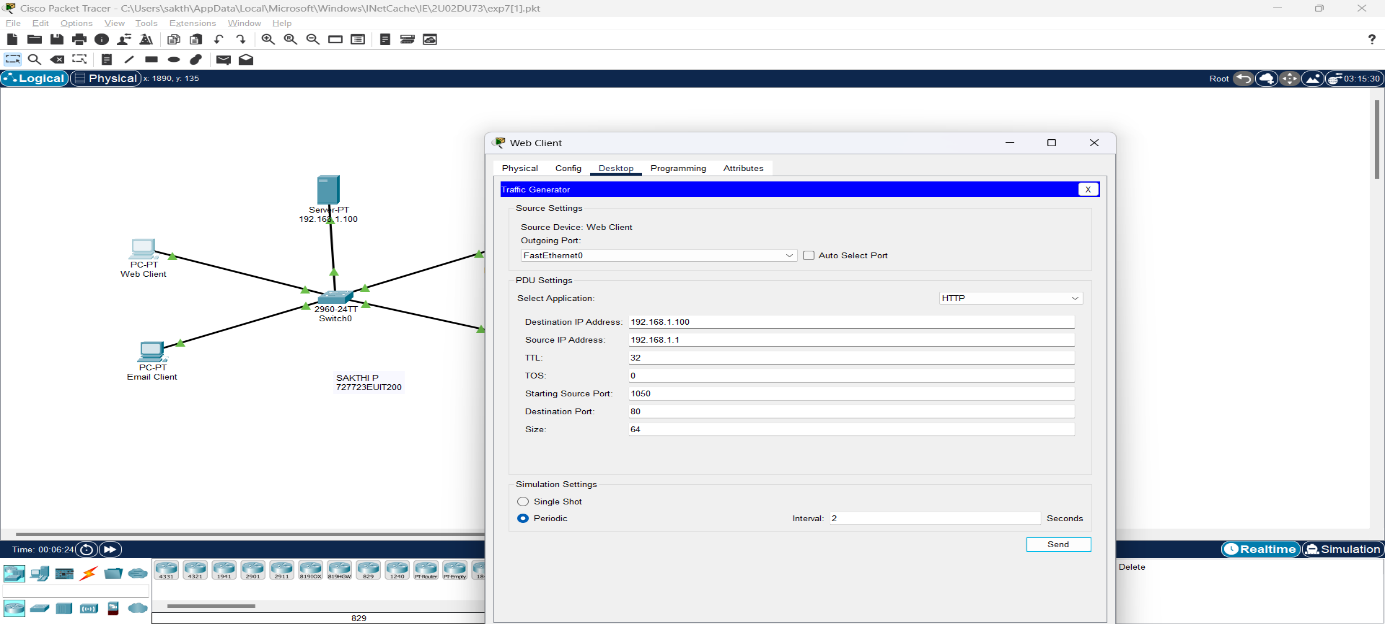
* Summarize key findings such as average latency, packet loss, or protocol overhead.
* Provide screenshots or logs of captured traffic for evidence.

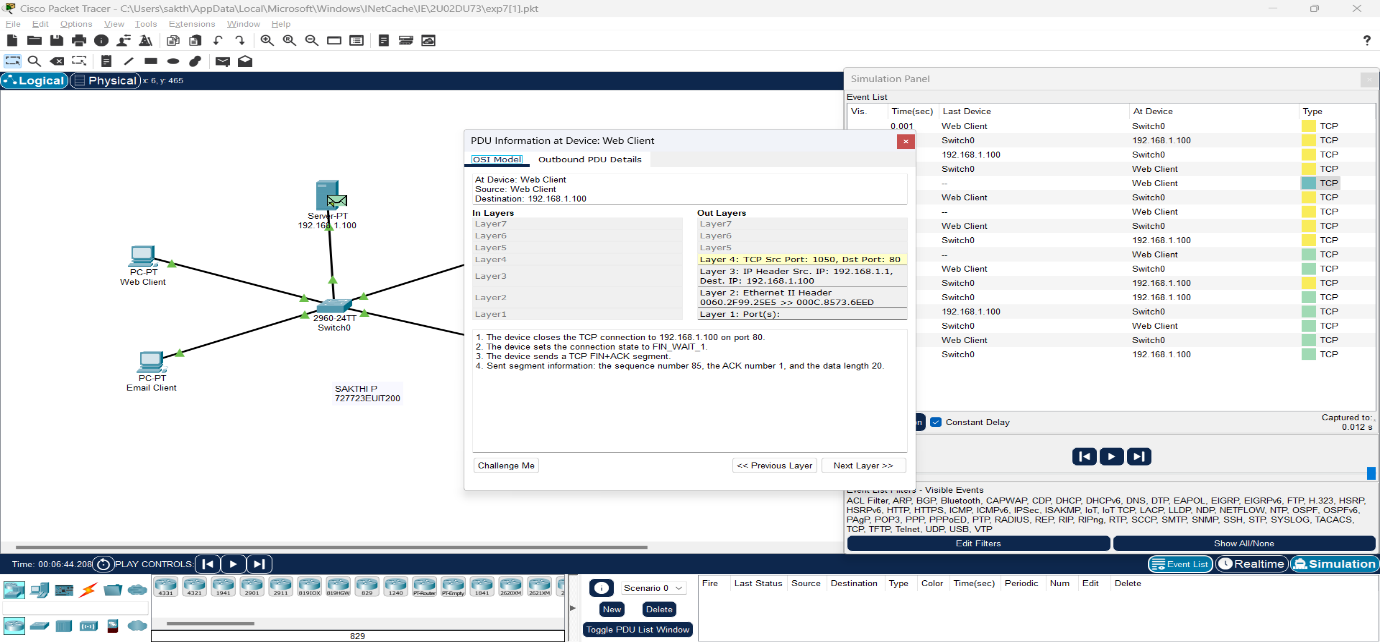
**Simulation screenshots:**

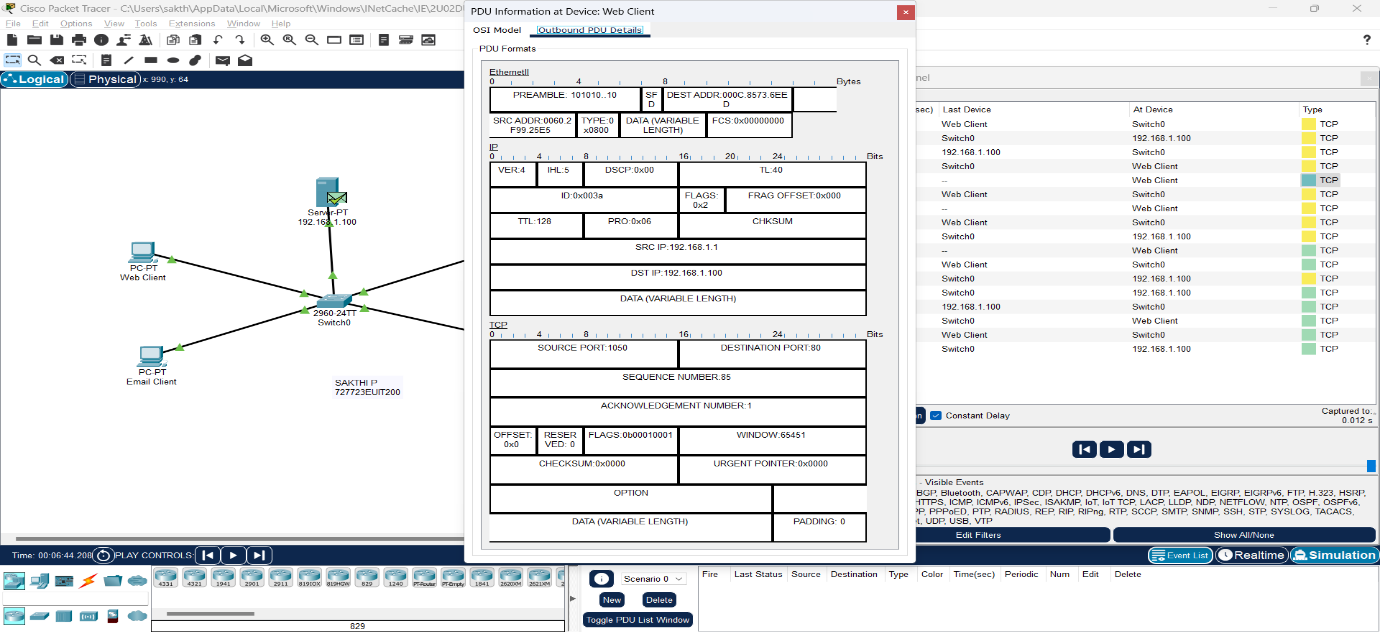


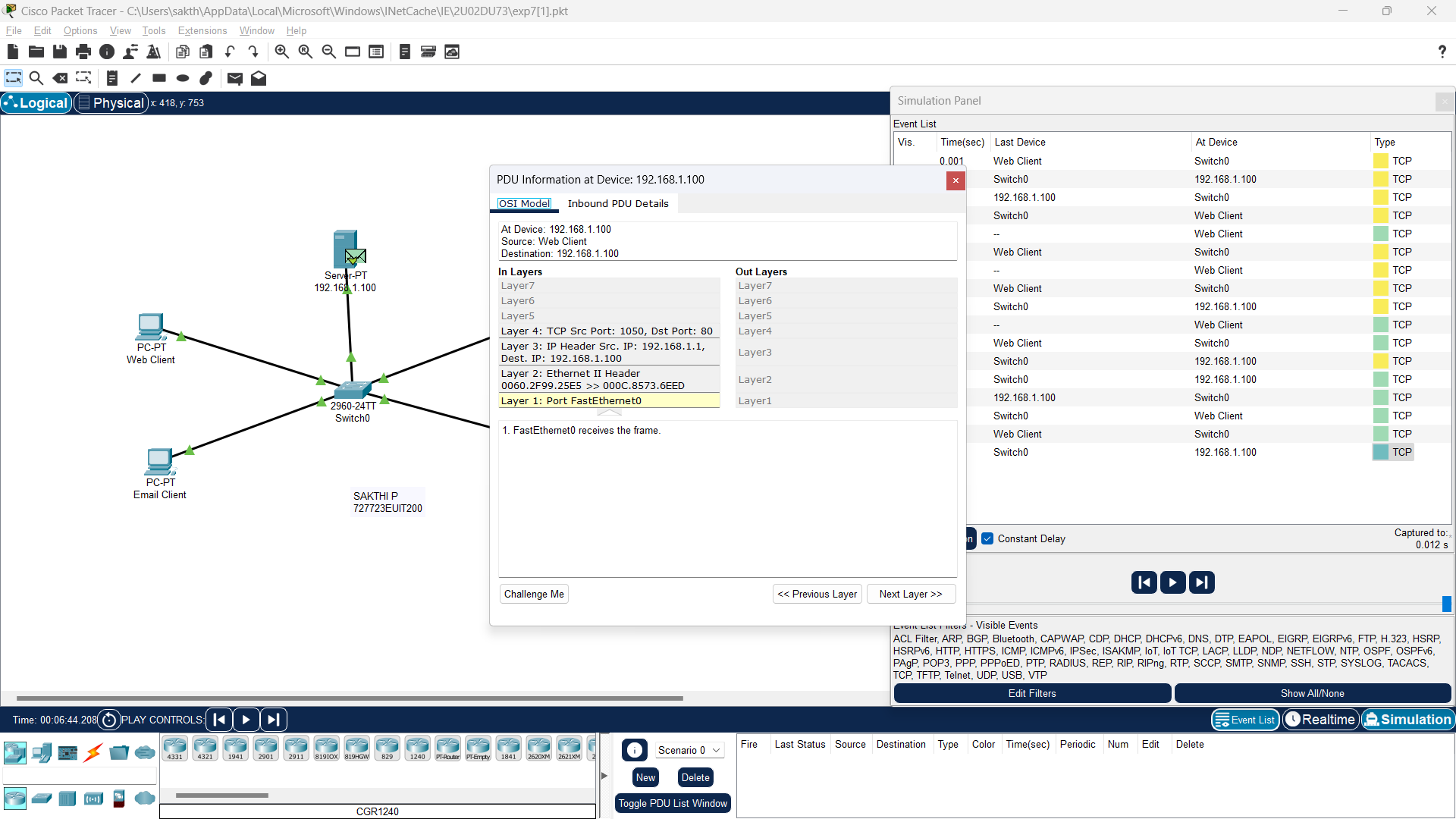


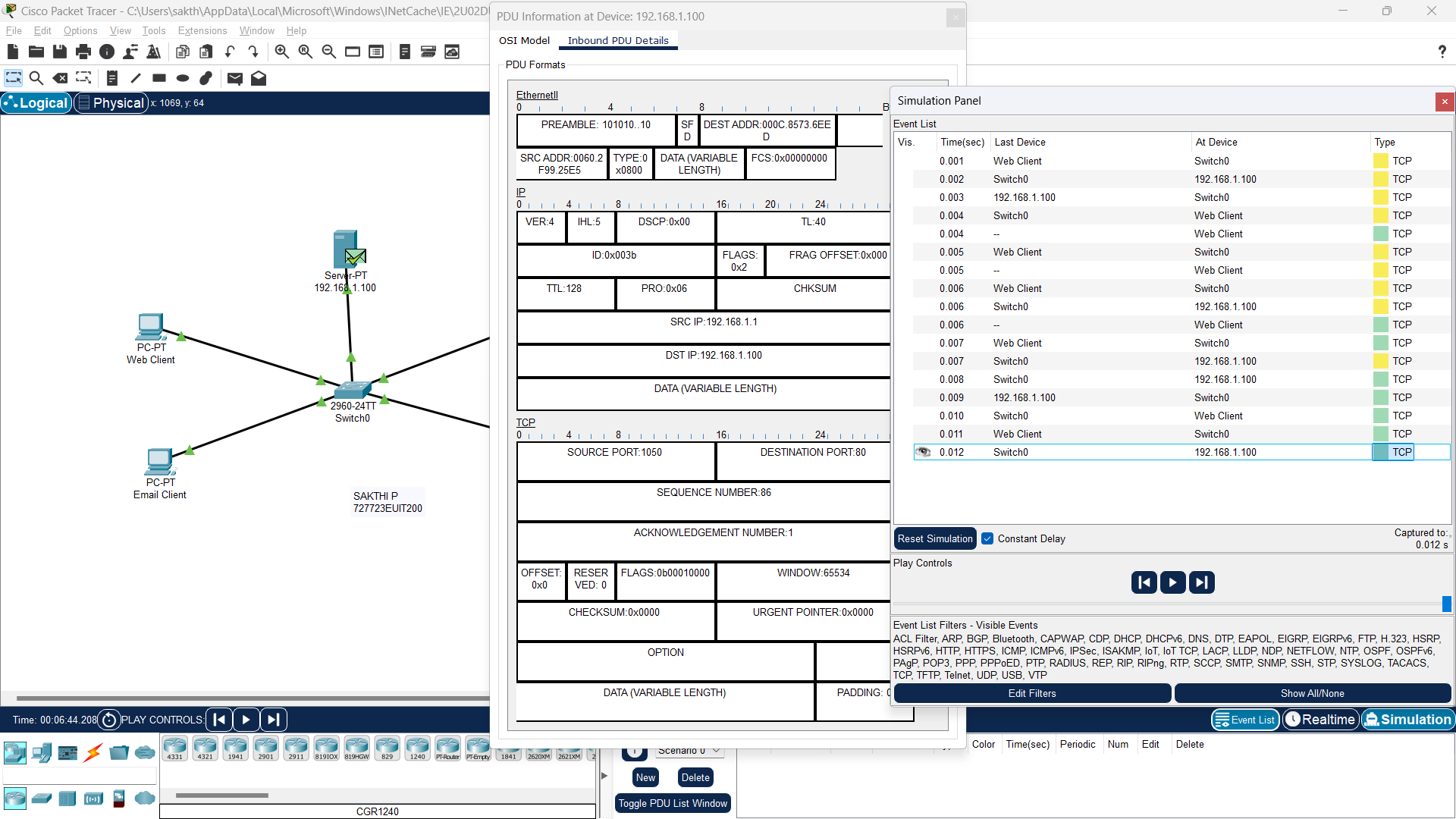


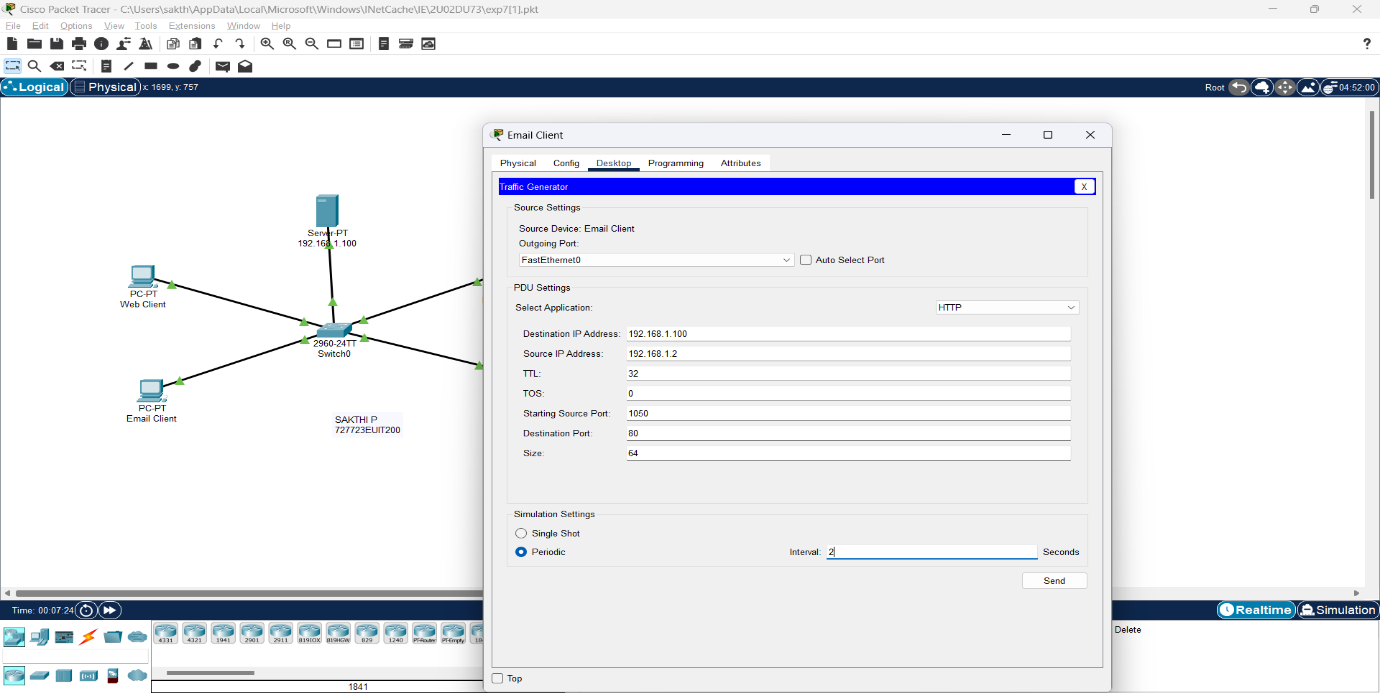


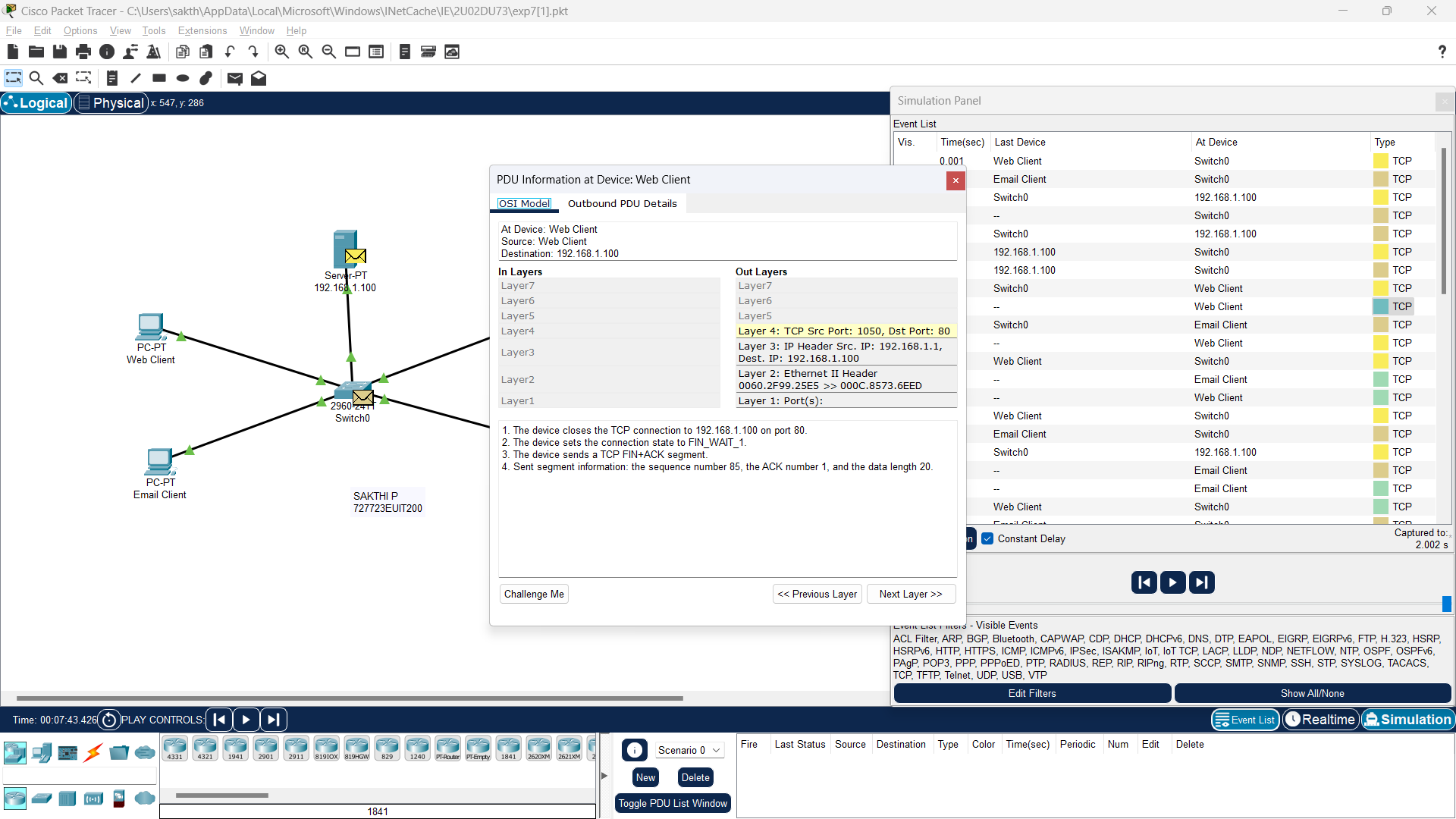


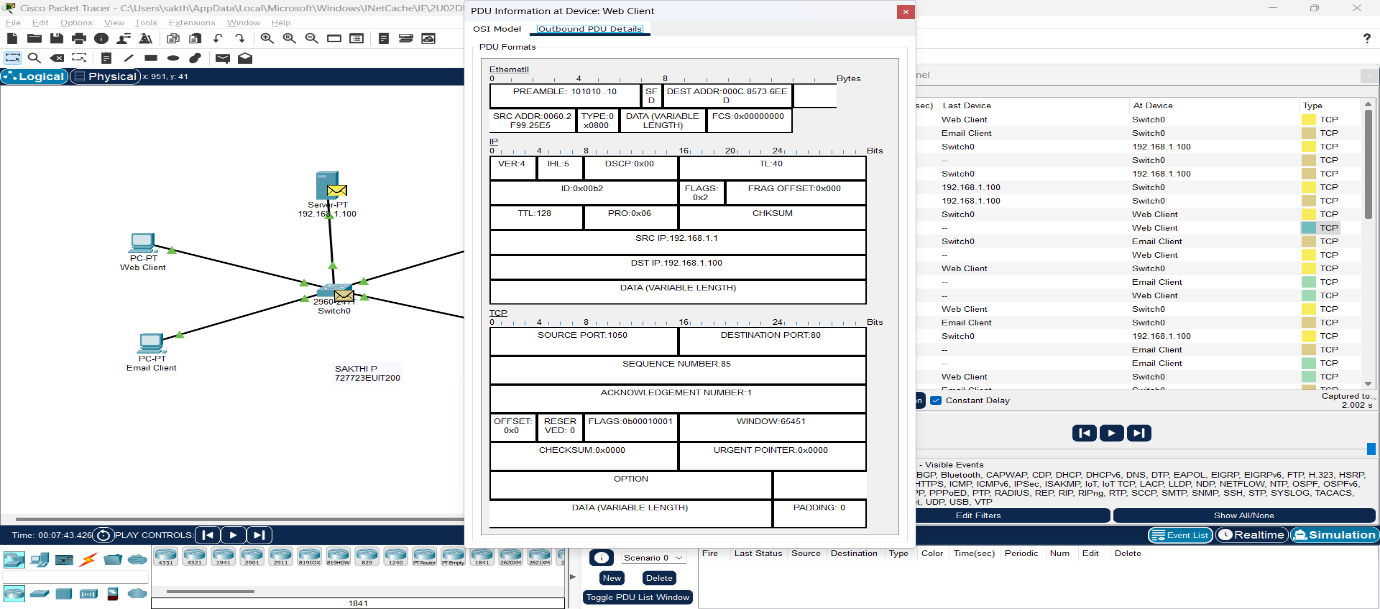


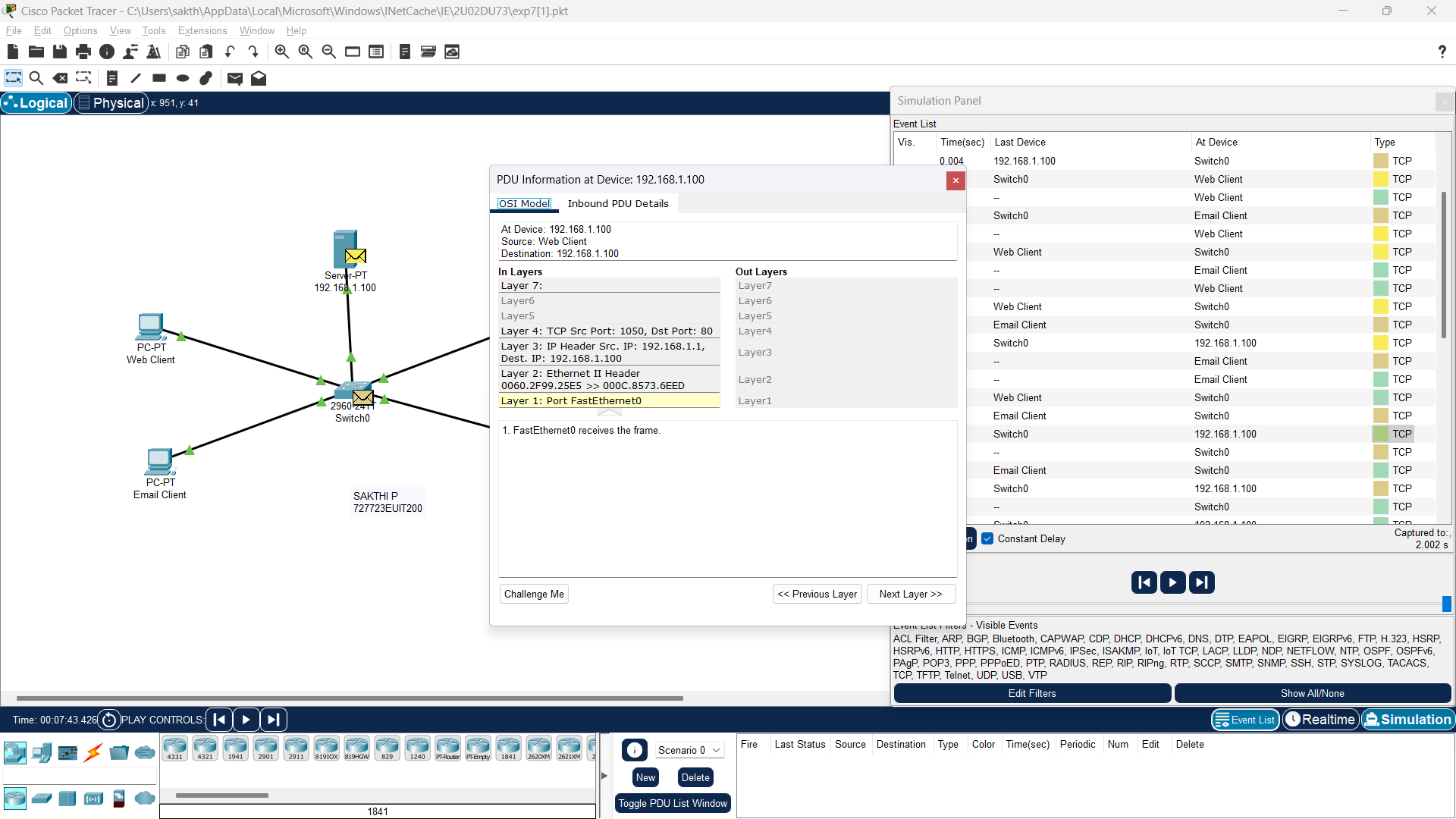


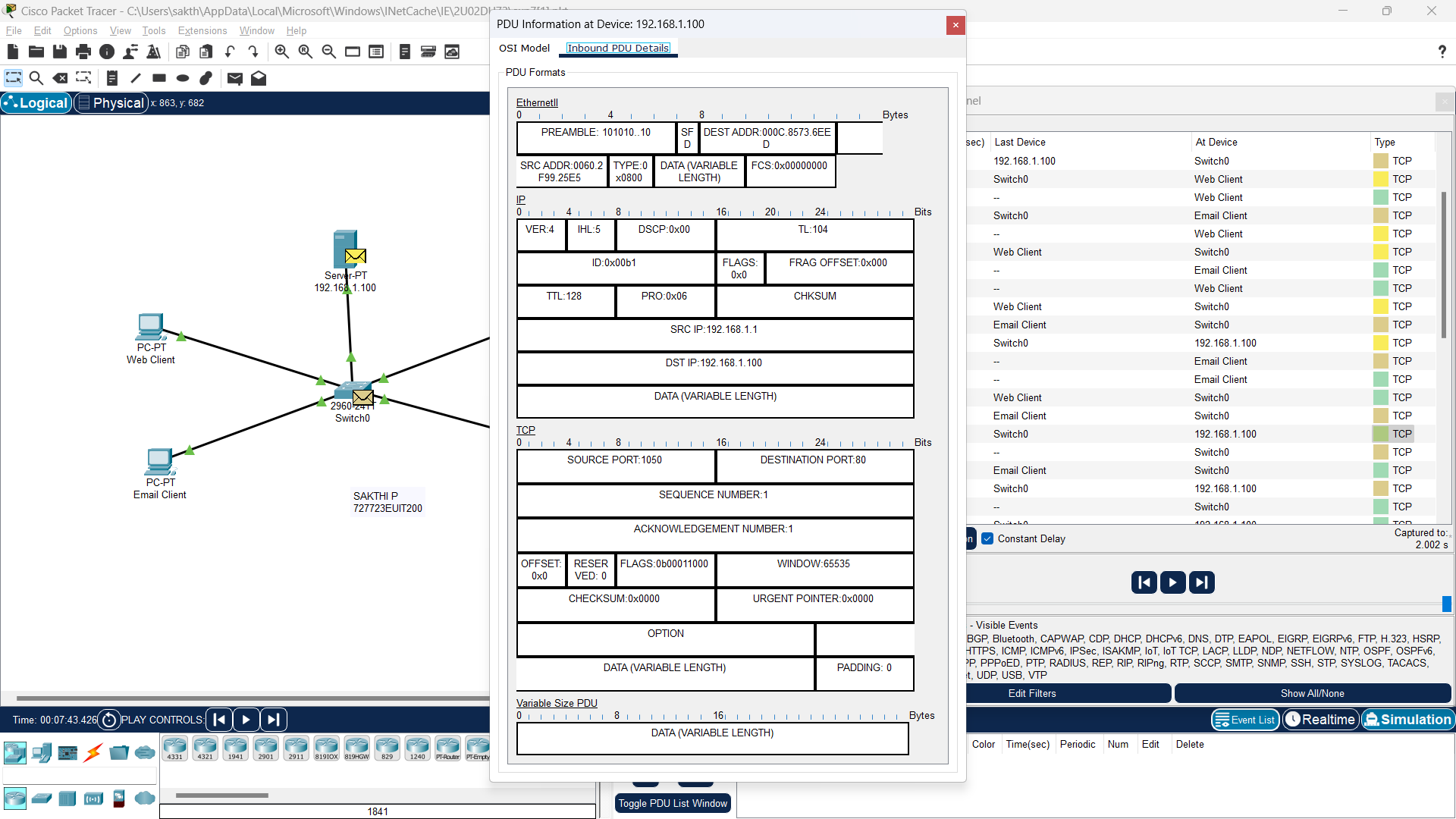


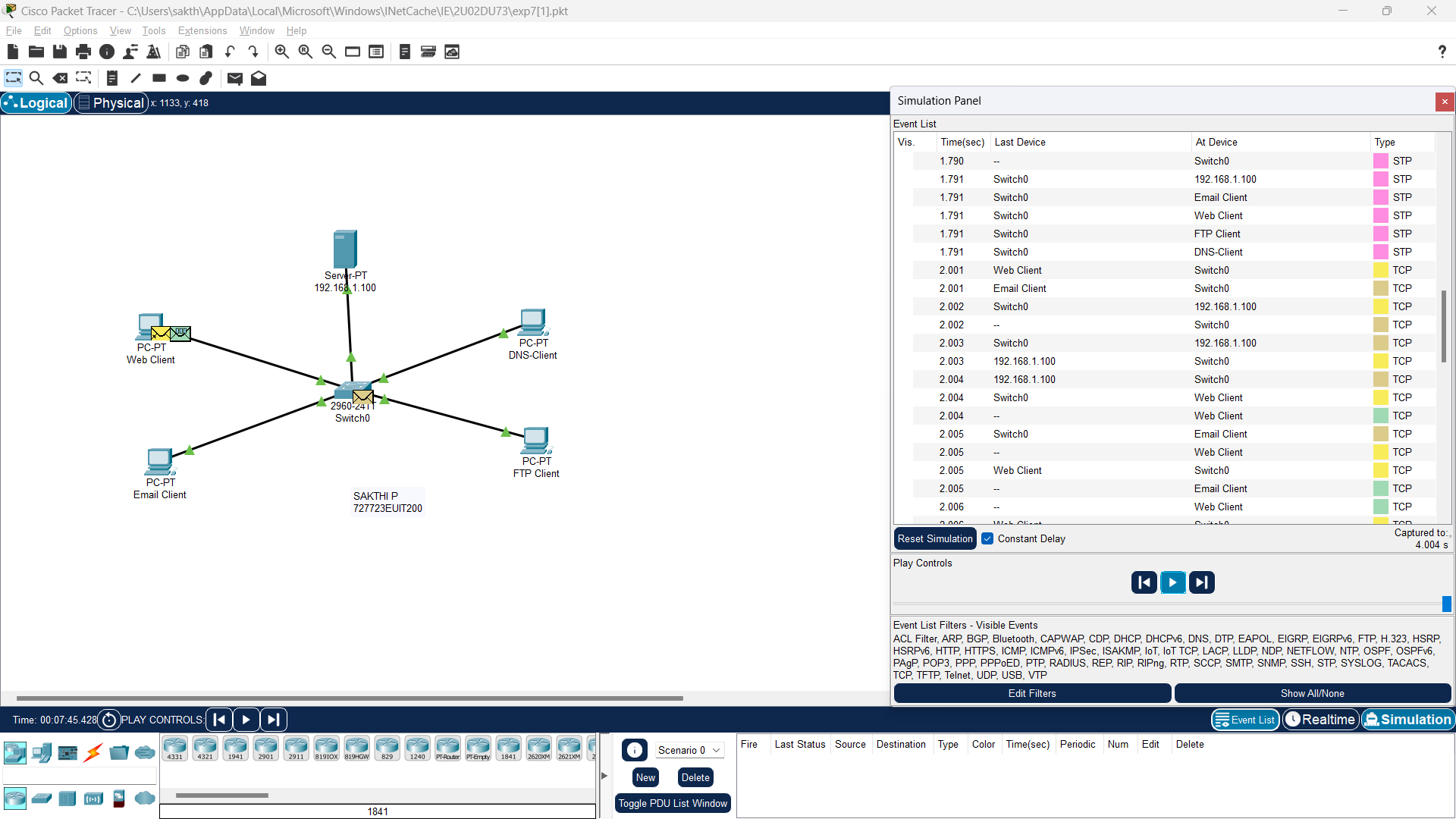












**Result:**

Thus, a simple LAN connection with server and four end users was simulated, HTTP application implemented in all 4 nodes, traffic generated in each node, one by one, for each node, and the network traffic analyzed for each step of transmission in simulation, using the Cisco Packet Tracer tool.