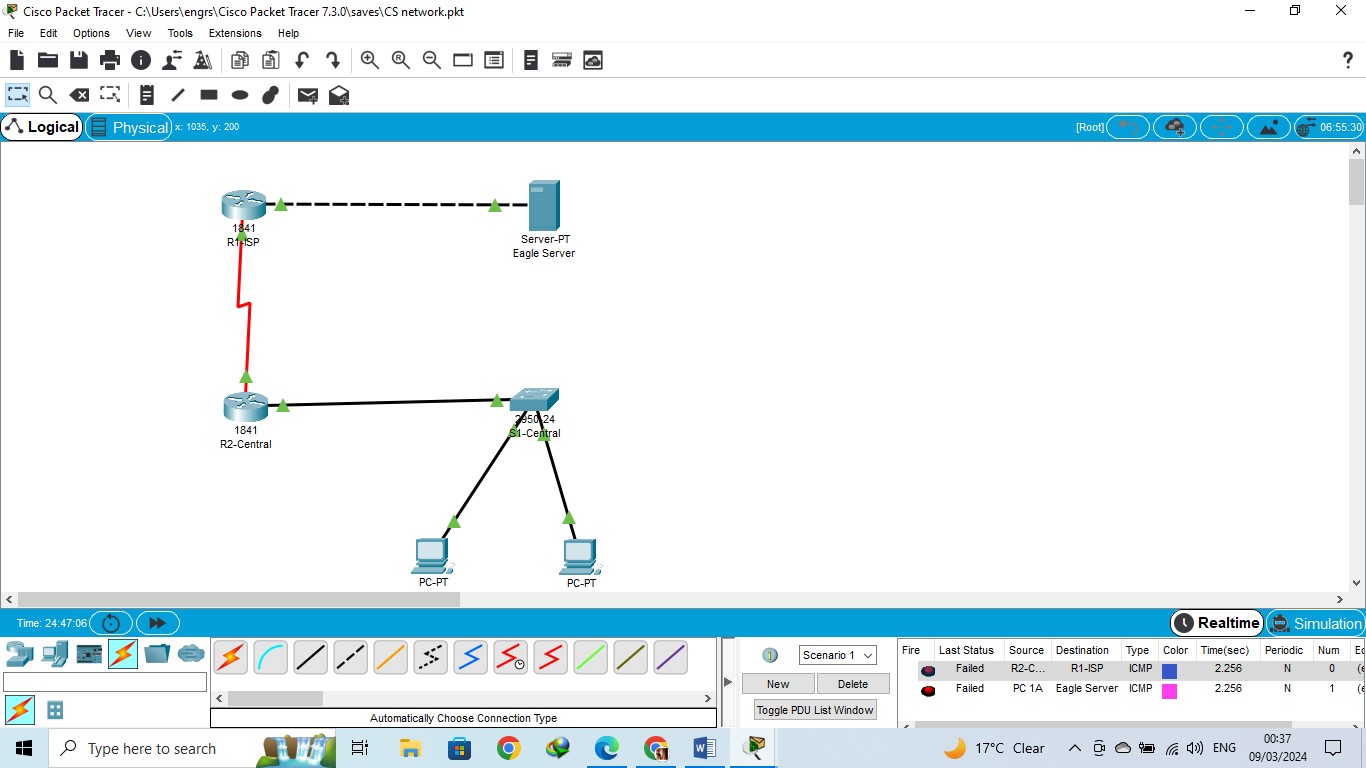
**Task 1: Build and analyse a standard topology**

In Packet Tracer, the process of network configuration encompasses the following steps: the assignment of IP addresses, the configuration of routing protocols, the activation of services, and the establishment of device connectivity.

This network has been created by following details provided in the lab 1.

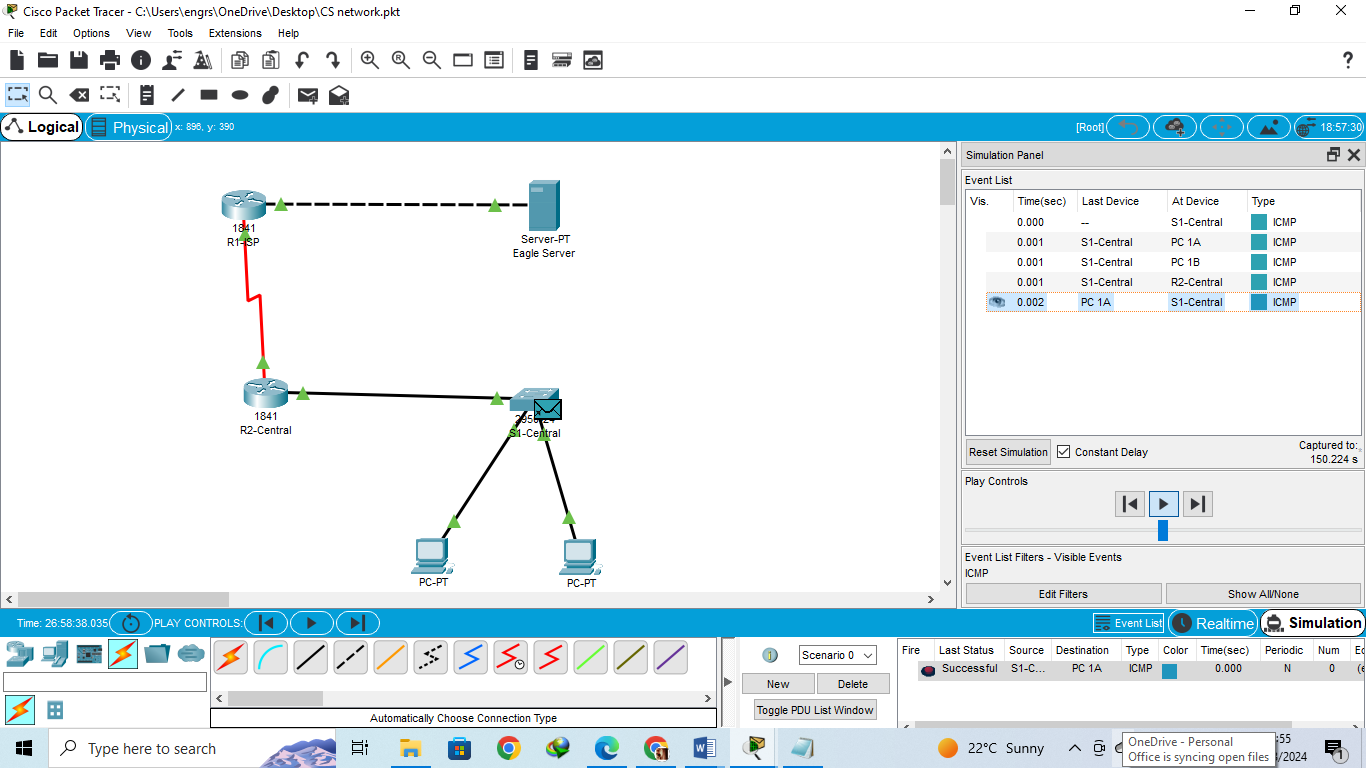


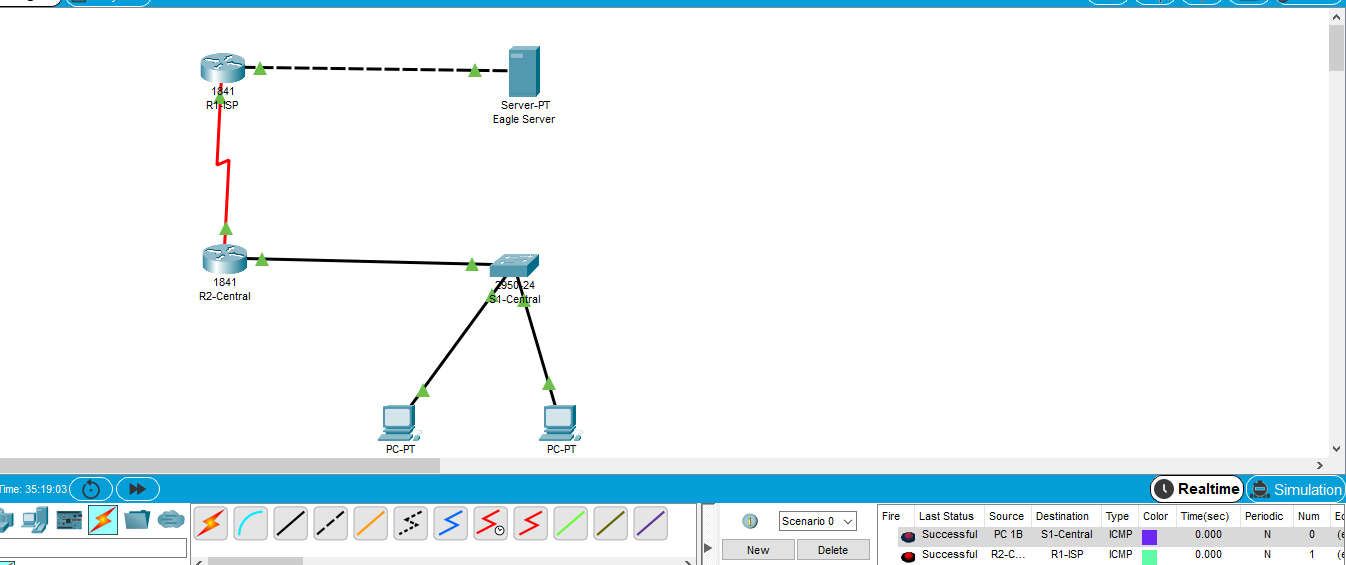
**Sending a simple PDU**

To view and assess Cisco Packet Tracer's Real-time Mode operation, perform these steps:   
  
**Check network configuration:**   
  
Check IP addresses, subnet masks, and routing settings to ensure can connect to the network.   
**Real-time availability**:   
  
Turn on Real-time Mode to use Packet Tracer.

**Select the source device:**   
  
Choose the device that will send the PDU. Two PCs, a switch, a server and two routers are used.

**Start PDU transfer:**   
  
Click on the device to send the PDU.  
Click on "Add Simple PDU" buttons on the device's UI or toolbar. Press it to generate a PDU.   
Simply follow the instructions to give the PDU the IP addresses, ports, and other needed information.

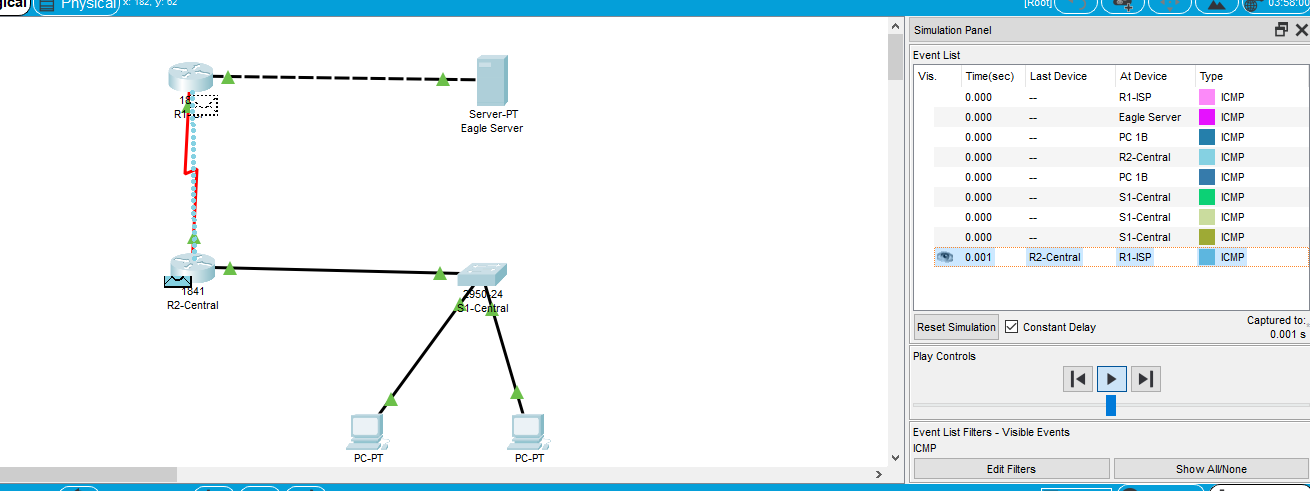




**2: Communication between PC 1B and Eagle Server**

**The Steps in the Communication Process:**Using Packet Tracer, configure the network by following the instructions provided by the lab. Set up a connection between PC 1B and the Eagle Server, and check that both computers have the appropriate IP addresses.   
  
Starting an ICMP Ping requires connecting to the Eagle Server's IP address using the command prompt on PC 1B. This will allow you to begin the process. It is possible to discover a server's IP address by pinging it.   
  
The Eagle Server collects an ICMP ping packet that was produced by PC 1B. This is the beginning of the data transfer process.   
  
One of the ICMP ping packets has been received by the Eagle Server.   
  
In the event that the Eagle Server is set up to react to ICMP ping requests, it will produce an ICMP echo reply packet as a response to the request.   
  
The ICMP echo reply packet is received by PC 1B using the network's data transfer infrastructure.   
  
PC 1B has successfully obtained the ICMP echo reply packet using the received packet.

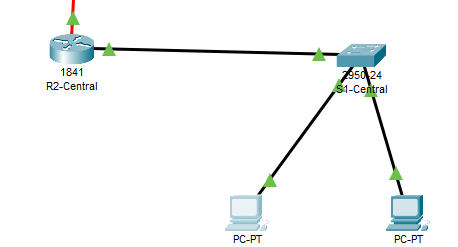
**Kind of package and the total number of steps:**   
  
An ICMP Echo Request packet, which is Type 8, is the type of packet that is transmitted during an ICMP ping operation. For the purpose of providing a response, the Eagle Server transmits a Type 0 ICMP Echo Reply packet.   
  
In most cases, the ICMP ping technique is comprised of the following four steps: PC 1B is responsible for transmitting ICMP Echo Request packets directly to the Eagle Server, which subsequently receives them. Following that, PC 1B generates and transmits the ICMP Echo Reply packets back to PC 1B from the Eagle Server. PC 1B then receives these packets for further processing.



**3: Looking inside Packets in simulation**

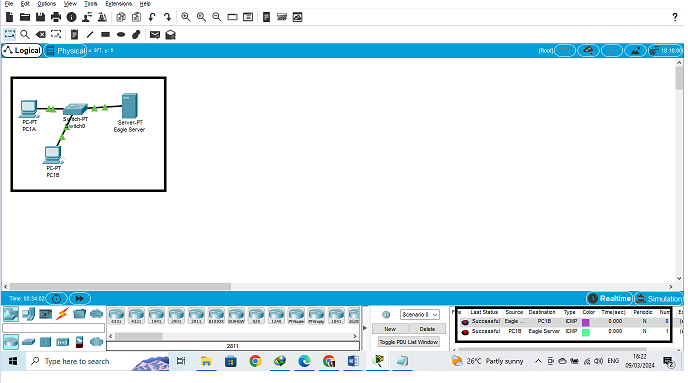
Combinations

* Switch-Router Combination



Using Packet Tracer, perform the procedure of connecting a switch and a router. Make certain that they are linked and configured in the appropriate manner.   
  
Construct a straightforward Protocol Data Unit (PDU) on a device that is connected to the switch via the switch. A personal computer that is connected to the switch is one example of this situation.   
  
Transmission: The Protocol Data Unit (PDU) is transmitted from the switch to the router in accordance with the Media Access Control (MAC) address of the destination.   
  
When it comes to Layer 2 analysis, the Protocol Data Unit (PDU) that is being received by the router has the MAC address of the switch's port as the source address, and the MAC address of the router's port as the destination address. Within the Protocol Data Unit (PDU) that is located at Layer 3, the Internet Protocol (IP) addresses of both the source and destination devices are kept secure.   
  
Routing: During the routing decision process, the router looks at the Layer 3 data, notably the IP addresses, in order to identify which interface is the outgoing interface.   
  
The router is responsible for transmitting the PDU from the appropriate interface to the location that it is meant for.   
  
Layer 2 Analysis: When the PDU is transmitted outward, the router's MAC address is now included as the source MAC address. Additionally, the MAC address of the device that comes after the router is included as the destination MAC address because of the Layer 2 analysis.   
  
Reception: After the Power Distribution Unit has successfully arrived at its intended destination, which may be another device that is connected to a router, the reception process begins.

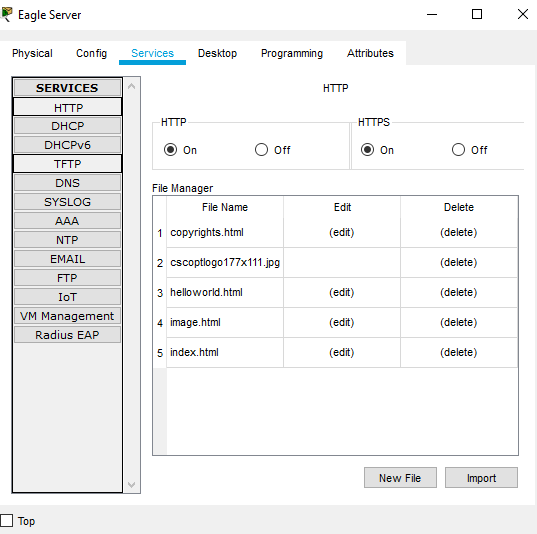
* PC-Server Combination



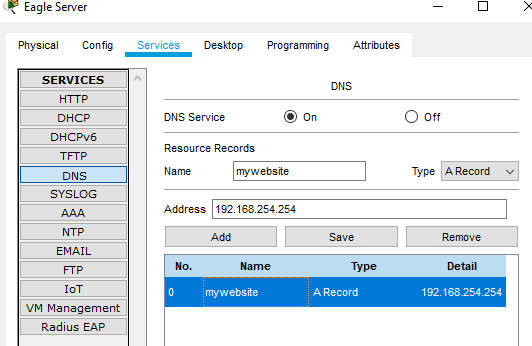
Setup: Connecting a PC to a server is required in order to set up Packet Tracer. Check to see that the devices have been correctly connected and set up.   
  
Generating PDU: One way to make a PDU is to use a computer to create a basic PDU.   
  
Transmission: The personal computer sends the portable data unit (PDU) to the server by referring to the server's IP address.   
  
It has been determined through the second layer of analysis that the MAC addresses of the source and destination of incoming PDUs that are sent to the server are the same as the MAC addresses of the network interfaces of the personal computer and the server, respectively. The packet delivery unit (PDU) at Layer 3 stores the Internet Protocol (IP) addresses of the devices that are sending and receiving data.   
  
The information included in the PDU is processed by the server after it has received the PDU notification.   
  
In such a scenario, the server might produce a response packet data unit (PDU).   
  
During transmission, the server will transmit the answer PDU back to the personal computer.   
  
Layer 2 Analysis: The response packet data unit (PDU) that is sent out by the server contains both the destination MAC address of the personal computer and the source MAC address of the server. This is an example of Layer 2 analysis.   
  
Reception: The PC receives the answer PDU as soon as it is returned to the server.

**4: DNS request from PC 1B to Eagle Server**

**Turn on HTTP Service:**



**Configure DNS service in the Eagle Server:**



**Click on the Web Browser from desktop:**

****

**Packet Types**

In the process of making a request for HTTP, a Type 6 TCP packet is employed, whereas DNS requests are carried out with Type 17 UDP packets. There are differences in the sorts of packets that are used by ICMP, HTTP, and DNS, which is a reflection of the underlying protocols that govern the processes of communication **(**Evensen, 1989**)**. For the purpose of determining whether or not a device is connected, diagnostics depend heavily on lightweight ICMP packets such as Echo Request and Echo Reply. HTTP packets, which are transmitted over TCP and divide requests and responses into a large number of packets, are responsible for ensuring the reliability of data transfer during web browsing (Jabi, 2016). These packets offer error detection, retransmission, and delivery in an ordered fashion (Jajodia, 2005). On the other hand, when using UDP to perform domain name resolution using single-packet queries and answers, DNS packets give priority to efficiency and speed over reliability (Moroni, 2005). It is imperative that network managers are aware of these distinctions in order to achieve maximum efficiency and accurately diagnose problems (Davies, 2022)ss.   
  
  
Conclusion: This task used Packet Tracer to examine network design events. We investigate protocols like ICMP, TCP, and UDP, as well as device and packet communication. These simulations increased the understanding of network communication (Jajodia, 2005). The session’s simulated data transfer between PCs, servers, switches, and routers. Network configuration, debugging, and optimisation need understanding packet types, protocols, and transmission and reception. Packet Tracer helps network managers understand their networks' activity, assuring their efficacy and stability (Moroni, 2005).

References

Evensen, P., & Dokken, T. (1989). Experiences using adjacency analysis for building topology structures. In *Theory and practice of geometric modeling* (pp. 419-432). Berlin, Heidelberg: Springer Berlin Heidelberg.

Jabi, W. (2016). Linking design and simulation using non-manifold topology. *Architectural Science Review*, *59*(4), 323-334.

Jajodia, S., Noel, S., & O’berry, B. (2005). Topological analysis of network attack vulnerability. *Managing Cyber Threats: Issues, Approaches, and Challenges*, 247-266.

Moroni, D., & Pascali, M. A. (2021). Learning topology: bridging computational topology and machine learning. *Pattern recognition and image analysis*, *31*(3), 443-453.  
  
Davies, T. (2022). Topological Data Analysis for Anomaly Detection in Host-Based Logs. *arXiv preprint arXiv:2204.12919*.