Data Communication and Networking

Project Report

(Assignment 04)

Group Members

Muhammad Zaki	**01-134231-068**
Humayun Tariq	**01-134231-028**

Department of Computer Science
Bahria University, Islamabad Campus

Abstract

This report provides a detailed explanation of the design and setup of a computer network for a hypothetical college environment. The design combines multiple network topologies—star, bus, ring, and mesh—to address diverse requirements. Subnetting is used to efficiently manage IP addresses, while the OSPF (Open Shortest Path First) protocol ensures seamless communication between the different local networks. Network analysis and troubleshooting are performed using tools like Cisco Packet Tracer.

Introduction

Modern organizations require networks that are flexible, efficient, and capable of addressing a variety of needs. This report focuses on creating a reliable network for a college campus, with different buildings using specific topologies tailored to their unique requirements. Subnetting ensures effective IP address allocation, while dynamic routing simplifies communication across subnets. The report also highlights how tools like Wireshark and Cisco Packet Tracer can help analyze and optimize the network's performance.

Cisco Packet Tracer

For design and development of the project, we will use Cisco Packet Tracer as our main tool. It is free and provided by Cisco. Cisco Packet Tracer is a comprehensive networking simulation software to create network topologies and imitate modern computer network. Packet tracer is very famous for its ease of use, simplicity, real time simulation and support for wide range of Cisco devices.

Reasons for using Cisco Packet Tracer

1. Following are some reasons for selecting Cisco Packet Tracer.

    - Cisco Packet tracker is designed for student who are learning networking.]
    - It’s simple and easy to use interface help student to learn network concepts and device configuration in a simple way.
    - It offers a drag and drop interface, which makes network design and development much easier for beginners.
    - Packet Tracer is less resources intensive as compared to other similar tools like GNS3.
    - It offers users to visualize network activities in real time and enhancing the understanding of packet flows and protocols.
    - It supports multiple network devices and protocols, making it a versatile option.
    - It supports the single and multi-users activities.

Advantages and Disadvantages of Cisco Packet Tracer

Advantages

- Easy to use (beginners friendly).
- Runs on low specification systems.
- Real time network packet and protocol visualization.
- Learning resources provided by Cisco itself on their online academy.
- Visualization of network activities really help you understand packet flow and protocols.

Disadvantages

- It only support cisco devices.
- Cannot stimulate operating system level tasks like GNS3 does.
- Lack the feature for advanced, large scale network stimulation.
- Lack the ability to stimulate some real word complexities of networks.

Comparison with Other Networking Simulation Tools

GNS3 vs Cisco Packet Tracer:

GNS3 offers more advanced capabilities, supporting real world network device images (IOS), able to perform task at operating system level which makes it ideal for larger much more complex and scale able system. It is also, more complex to set up and learning curve is much more steep as compared to the Packet Tracer and it requires significant computing power as compare to Packet Tracer which is not resources intensive. While Packet Tracer was designed for educational purposes and smaller network stimulation and it is much easier to use.

Cisco Packet Tracer		**GNS3**	
Advantages	**Disadvantages**	**Advantages**	**Disadvantages**
User friendly	Limited to Cisco network	Highly customizable	Steeper learning curve
Low resource requirement	Lacks full-scale real-world network	Support real world device images	High Resource demand
Real time simulation	Lack advance features	Real operating system simulation	Requires real device images

EVE-NG vs Cisco Packet Tracer

EVE-NG is designed for professionals working in multi-vendor scenarios and support a range of vendor images while Packet Tracer only support Cisco devices. EVE-NG provides more professional grade simulation but it has higher complexity and higher resource demands.

Cisco Packet Tracer		EVE-NG	
Advantages	**Disadvantages**	**Advantages**	**Disadvantages**
User friendly	Limited to Cisco network	Real device emulation	Complex setup
Low resource requirement	Lacks full-scale real-world network	Support advance multi vendor scenarios.	Requires powerful hardware
Real time simulation	Lack advance features	Support collaboration	Designed for professionals.

NS3 vs Cisco Packet Tracer

NS3 is open source and its code base tools are much more suited for large scale network research. While Cisco Packet Tracer is great for quick setup and learning, NS3 allow for in depth network performance analysis, making them more suited for research purposes.

Cisco Packet Tracer		NS3	
Advantages	**Disadvantages**	**Advantages**	**Disadvantages**
User friendly	Limited to Cisco network	Highly customizable	No GUI
Low resource requirement	Lacks full-scale real-world network	Suited for large scale research	Code based tools
Real time simulation	Lack advance features	Great for performance analysis	Should know C++/Python

Network Design

The network incorporates the following topologies:

- **Star Topology:** Utilized in administrative buildings to provide centralized control and easy management.
- **Bus Topology:** Deployed in older sections of the network to minimize costs while maintaining functionality.
- **Ring Topology:** Applied in computer labs where reliable and sequential data flow is critical.

- **Mesh Topology:** Implemented in critical areas to ensure redundancy and high availability.

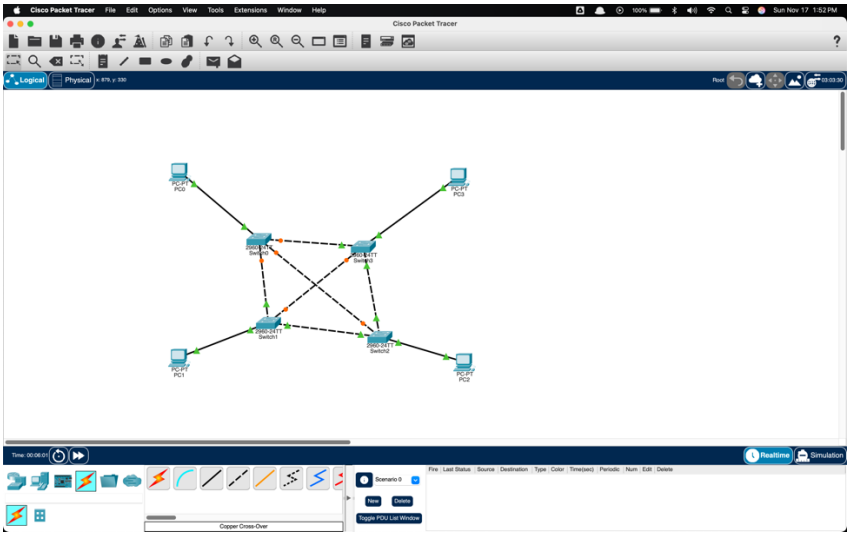
To make these topologies in Cisco Packet Tracer we will be using Switch and PC and Copper Straight and Cross Over for them.

For PC to switch connection we will be using Copper Straight through wire using Fast ethernet port both on PC and switch. For the connection between switches we used Copper Cros Over wire on Fast Ethernet port. Assigned IP to each PC according to our network.

Mesh Topology

In mesh topology, every device has dedicated point to point connection with other device, which allow much higher data transfer rate and privacy and it is quite robust.

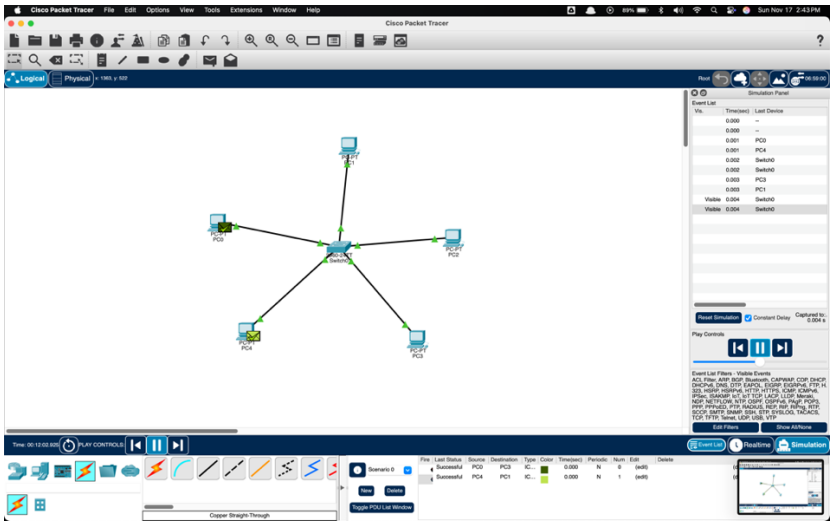
To design this topology in Cisco Packet Tracer, we will take 4 devices and we will use switches to establish connection with other devices in the network.



Star Topology

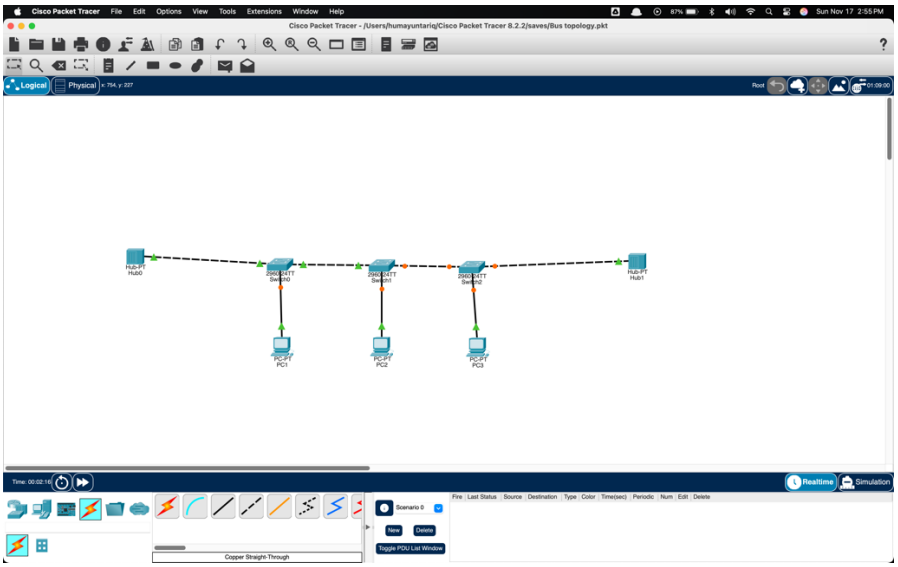
For star topology we will also use the one switch and 5 PC to make a star topology and the switch will act as central hub through which all PC will be connected to each other.

To test the network in simulation sending a sample message from PC0 to PC3 and PC4 to PC1. Once the message is received at the designation it will send back the acknowledgment to the source.



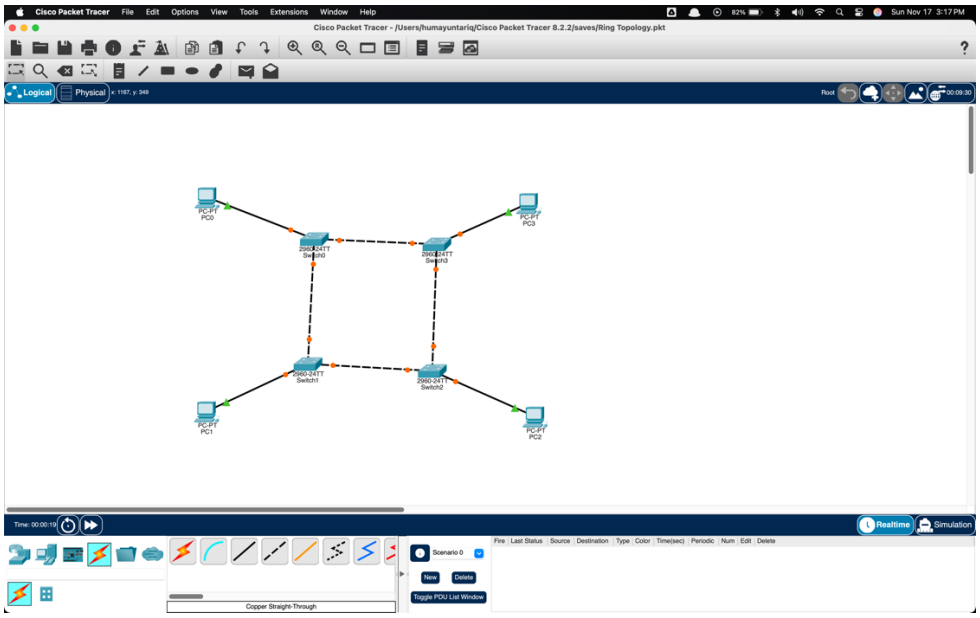
Bus Topology:

In bus topology, there are is a main cable along with different PC are connected. To design Bus topology in Cisco Packet Tracer we used hub on both end and a switches between them to make connect for the PCs.



Ring Topology:

In Ring Topology, every device have dedicated point to point connection with device on there left and right. So in Cisco Packet Tracer, we will use switches and PC to make this topology. The PC will have there own switches and they will connect to switched on right and left.



Complex Network Architecture

Network Addressing and Subnetting

Since each LAN doesn't have more 4 to 5 PC it will be much more good approach if we subnet the single IP, in this way the number of IP wasted will be very low.

To manage IP addresses efficiently, the network uses the 192.168.12.0/24 range, divided into 16 subnets. Each subnet has a subnet mask of 255.255.255.240, supporting up to 14 usable host addresses.

We can use the network and there host IP addresses range of 192.168.12.0/28 and 192.168.12.240/28.

Network ID	Host IP Addresses Range		Broadcast Address
	1st Host Address	Last Host Address	
192.168.12.0	192.168.12.1	192.168.12.14	192.168.12.15
192.168.12.16	192.168.12.17	192.168.12.30	192.168.12.31
192.168.12.32	192.168.12.33	192.168.12.46	192.168.12.47
192.168.12.48	192.168.12.49	192.168.12.62	192.168.12.63
192.168.12.64	192.168.12.65	192.168.12.78	192.168.12.79
192.168.12.80	192.168.12.81	192.168.12.94	192.168.12.95
192.168.12.96	192.168.12.97	192.168.12.110	192.168.12.111

192.168.12.112	192.168.12.113	192.168.12.126	192.168.12.127
192.168.12.128	192.168.12.129	192.168.12.142	192.168.12.143
192.168.12.144	192.168.12.145	192.168.12.158	192.168.12.159
192.168.12.160	192.168.12.161	192.168.12.174	192.168.12.175
192.168.12.176	192.168.12.177	192.168.12.190	192.168.12.191
192.168.12.192	192.168.12.193	192.168.12.206	192.168.12.207
192.168.12.208	192.168.12.209	192.168.12.222	192.168.12.223
192.168.12.224	192.168.12.225	192.168.12.238	192.168.12.239
192.168.12.240	192.168.12.241	192.168.12.254	192.168.12.255

Router and PC Configuration

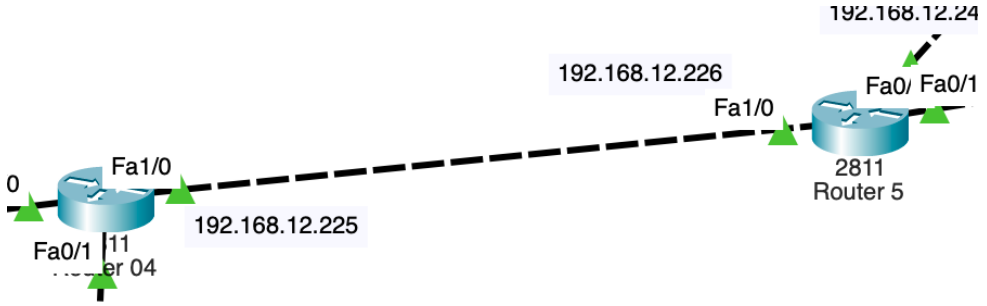
- Router Ports: The first IP address in each subnet is reserved for the router interface.
- PCs: Each PC is assigned the next available IP address in the subnet. The router's IP is used as the default gateway for the PCs.

Technologies For Network Architecture

- Routers (which have 4 Fast ethernet port, initially they have 2 but we add new 2 Fast Ethernet module to meet our port need, that will give us total of 4 fast ethernet ports on each router)
- Switches
- PCs

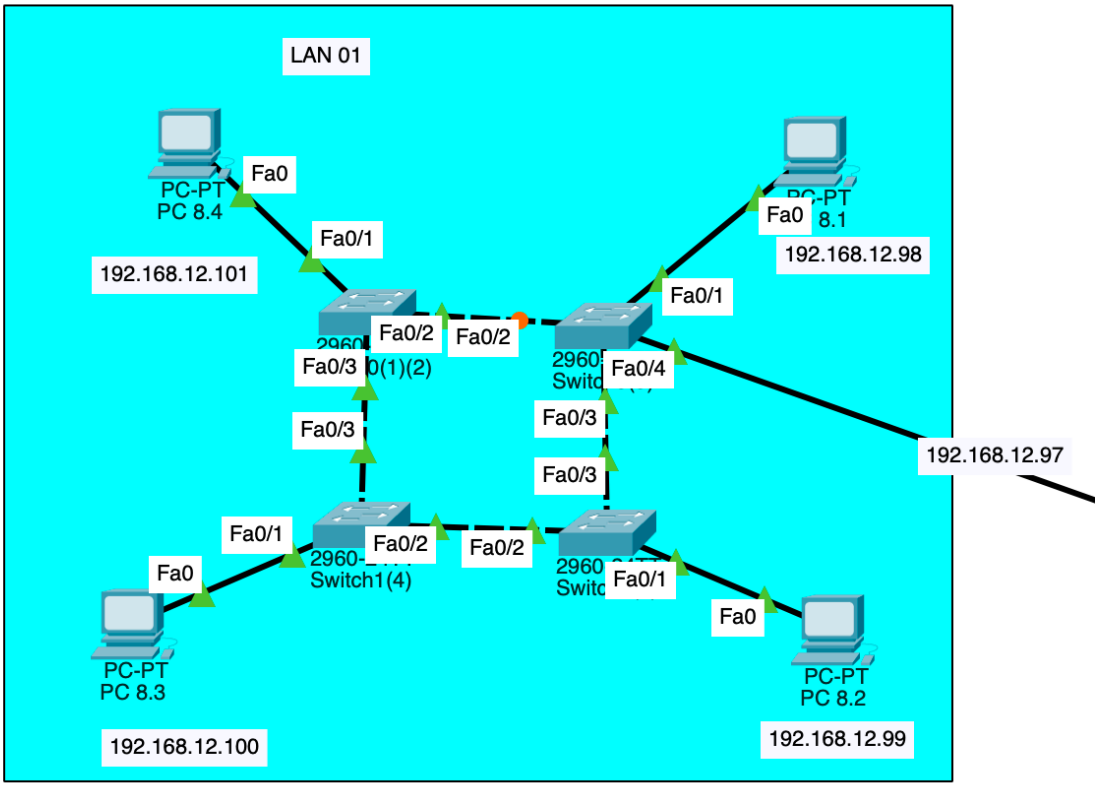
Network Design

For connecting router to router we will use a two addresses in a new network like 192.168.12.224. Lets take Router 4 and Router 5 we used 192.168.12.224 network and assigned 192.168.12.225 to Fast ethernet port f1/0 and 192.168.12.226 to Fast ethernet port f1/0. We will do the same for every connection in the between routers.



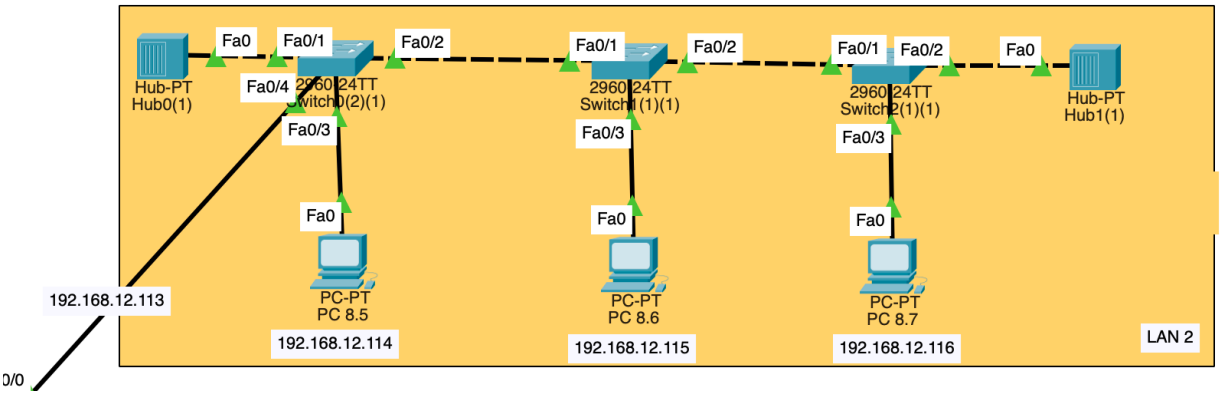
LANS:

LAN 01:



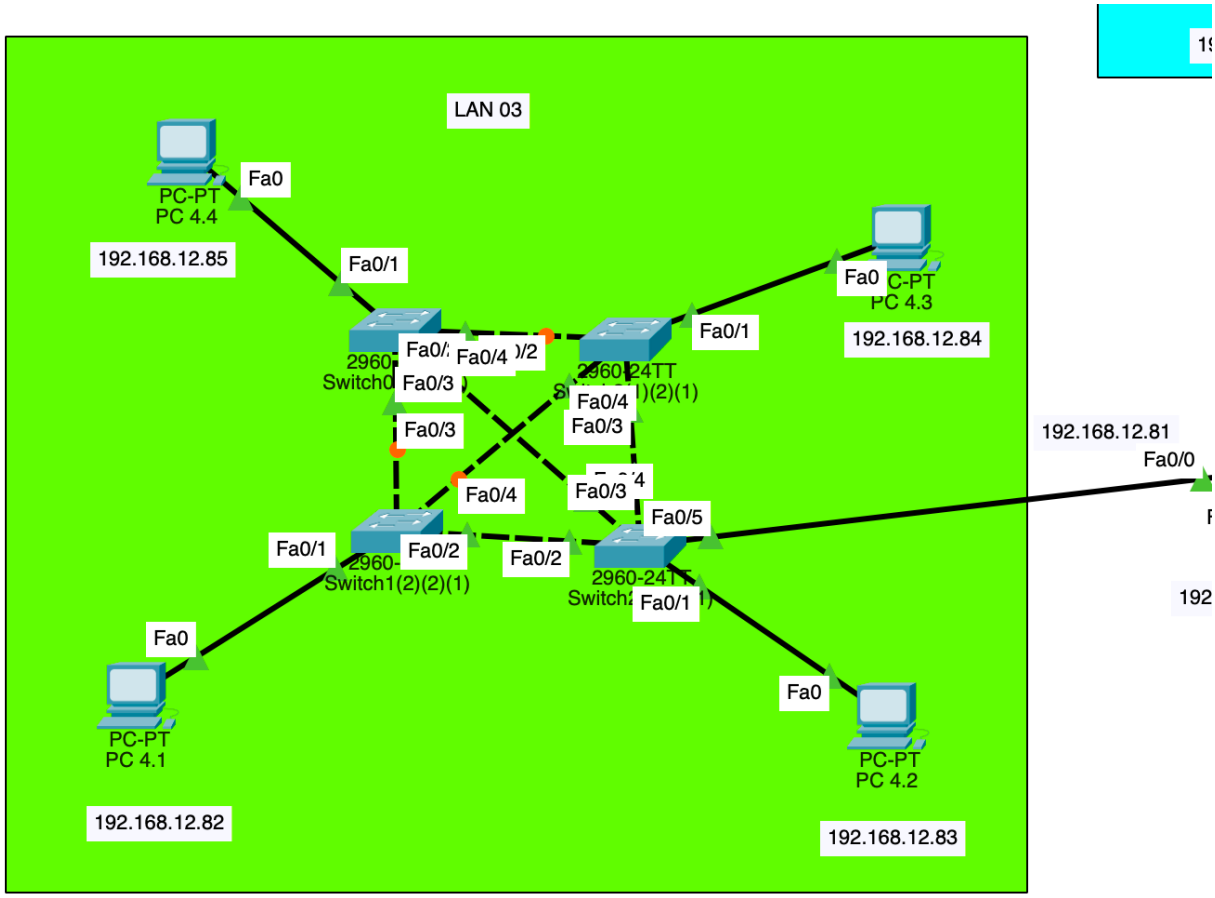
In LAN 01, we are using 192.168.12.96/28 sub-network, the first IP is assigned to Router 192.168.12.97/28 and there are 4 PC 192.168.12.98/28 - 192.168.12.101/28 will be assigned to PCs.

LAN 02:



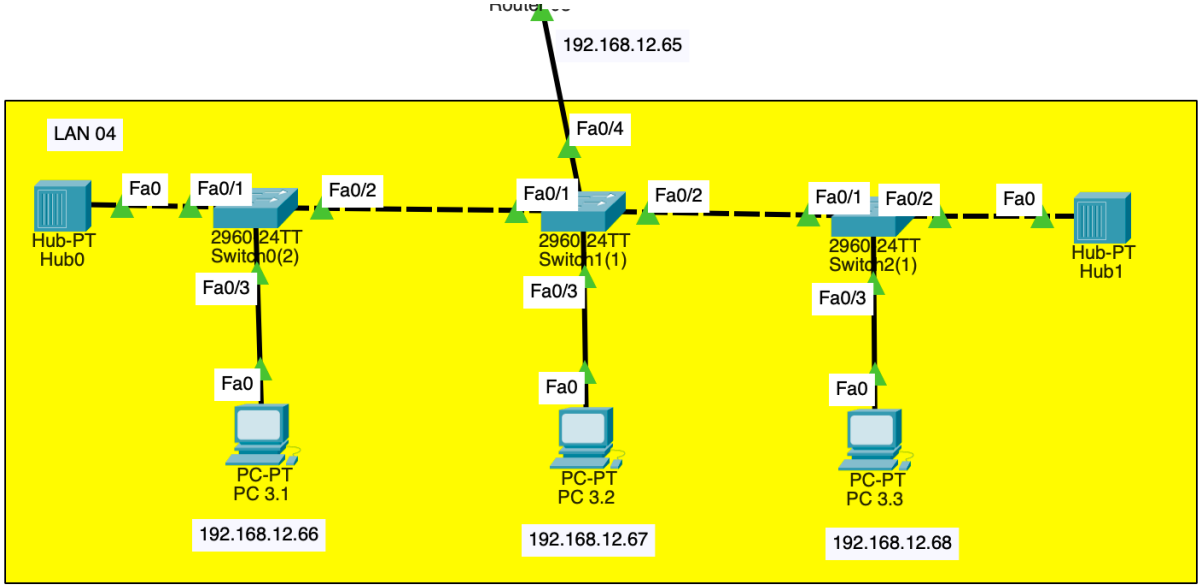
In LAN 02, we are using 192.168.12.112/28 sub-network, the first IP is assigned to Router 192.168.12.113/28 and there are 3 PCs 192.168.12.114/28 - 192.168.12.116/28 will be assigned to PCs.

LAN 03:



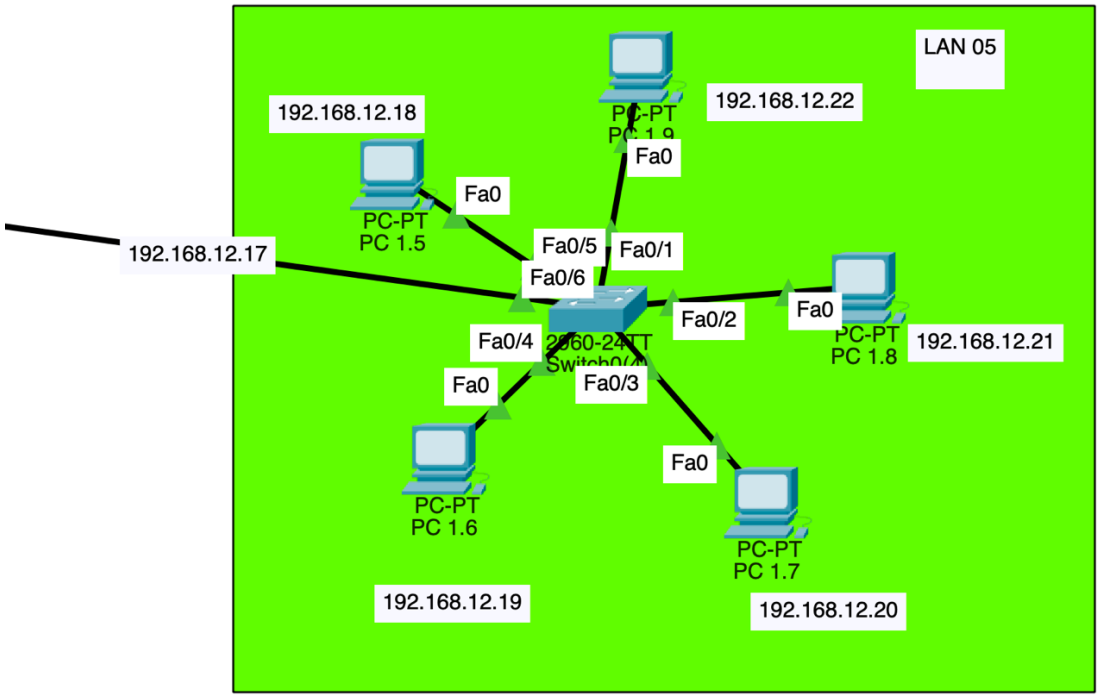
In LAN 03, we are using 192.168.12.80/28 sub-network, the first IP is assigned to Router 192.168.12.81/28 and there are 4 PCs 192.168.12.82/28 - 192.168.12.85/28 will be assigned to PCs.

LAN 04:



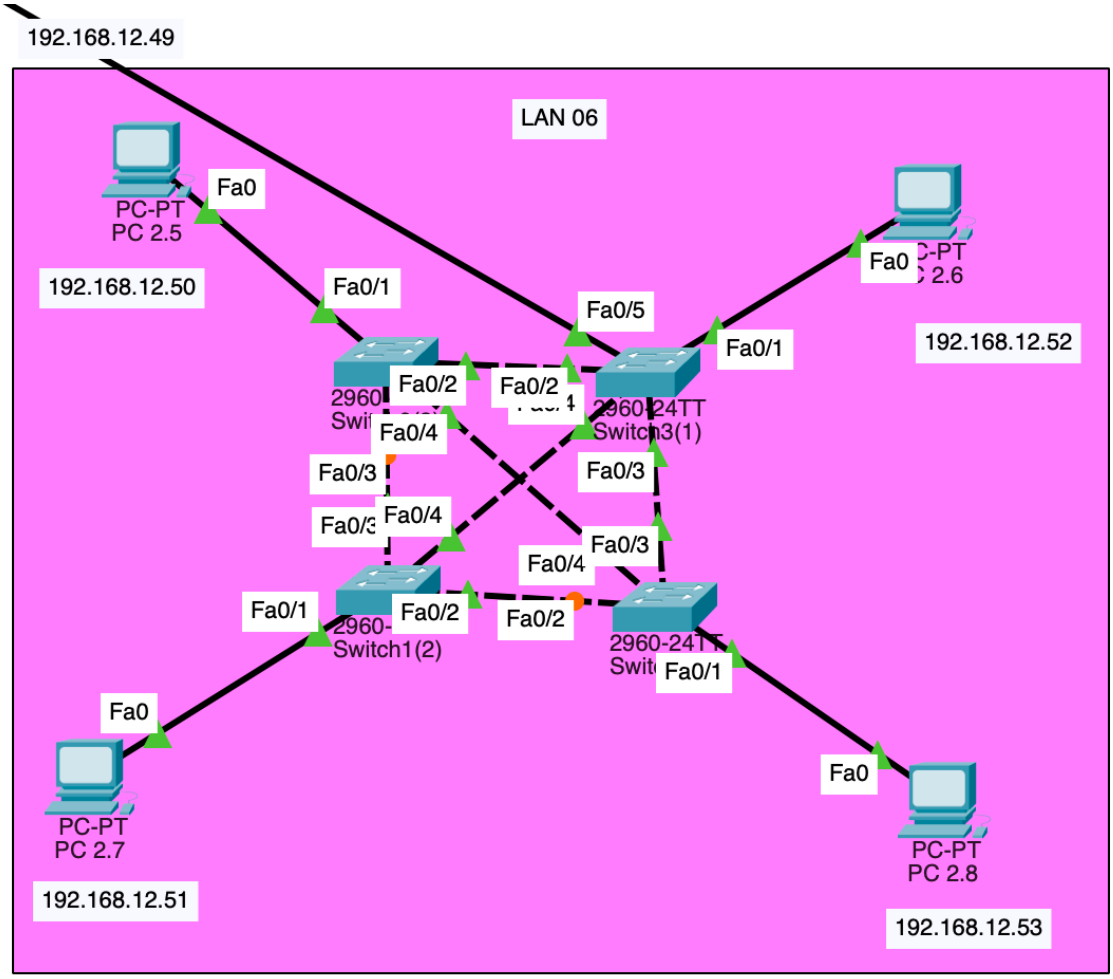
In LAN 04, we are using 192.168.12.64/28 sub-network, the first IP is assigned to Router 192.168.12.65/28 and there are 3 PCs 192.168.12.66/28 - 192.168.12.68/28 will be assigned to PCs.

LAN 05:



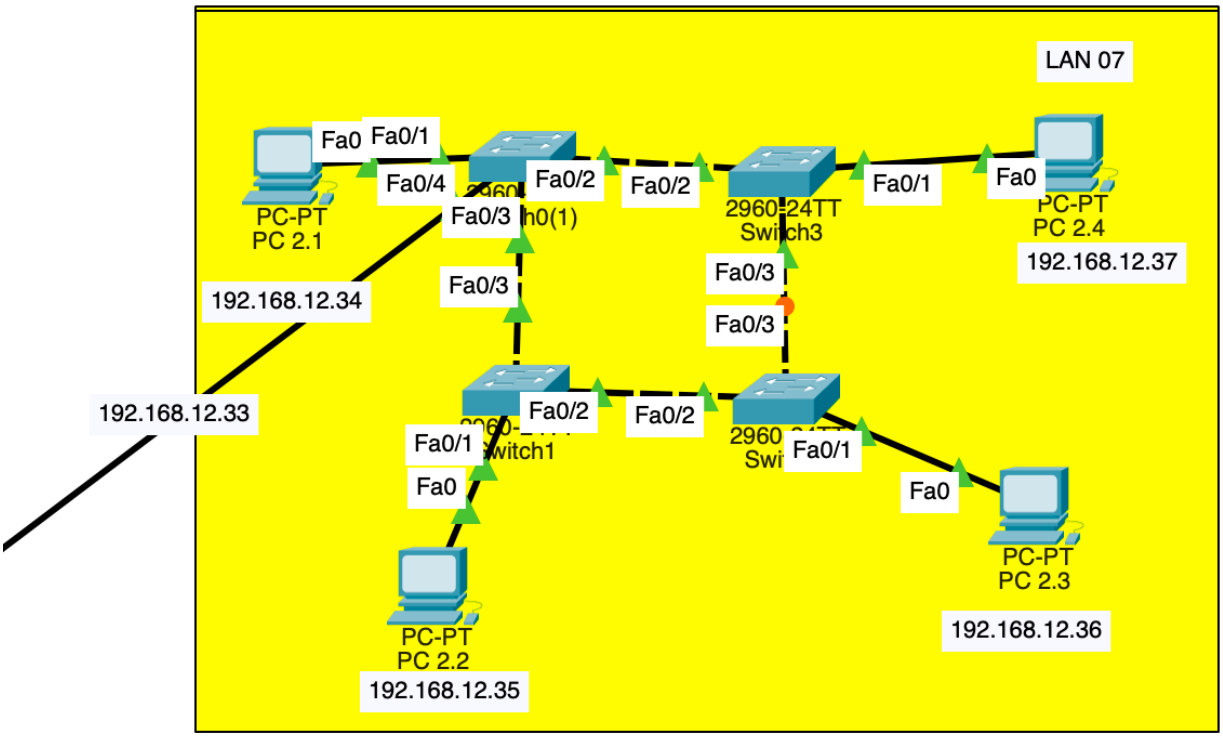
In LAN 05, we are using 192.168.12.16/28 sub-network, the first IP is assigned to Router 192.168.12.17/28 and there are 5 PCs 192.168.12.18/28 - 192.168.12.22/28 will be assigned to PCs.

LAN 06:



In LAN 06, we are using 192.168.12.48/28 sub-network, the first IP is assigned to Router 192.168.12.49/28 and there are 4 PCs 192.168.12.50/28 - 192.168.12.53/28 will be assigned to PCs.

LAN 07:



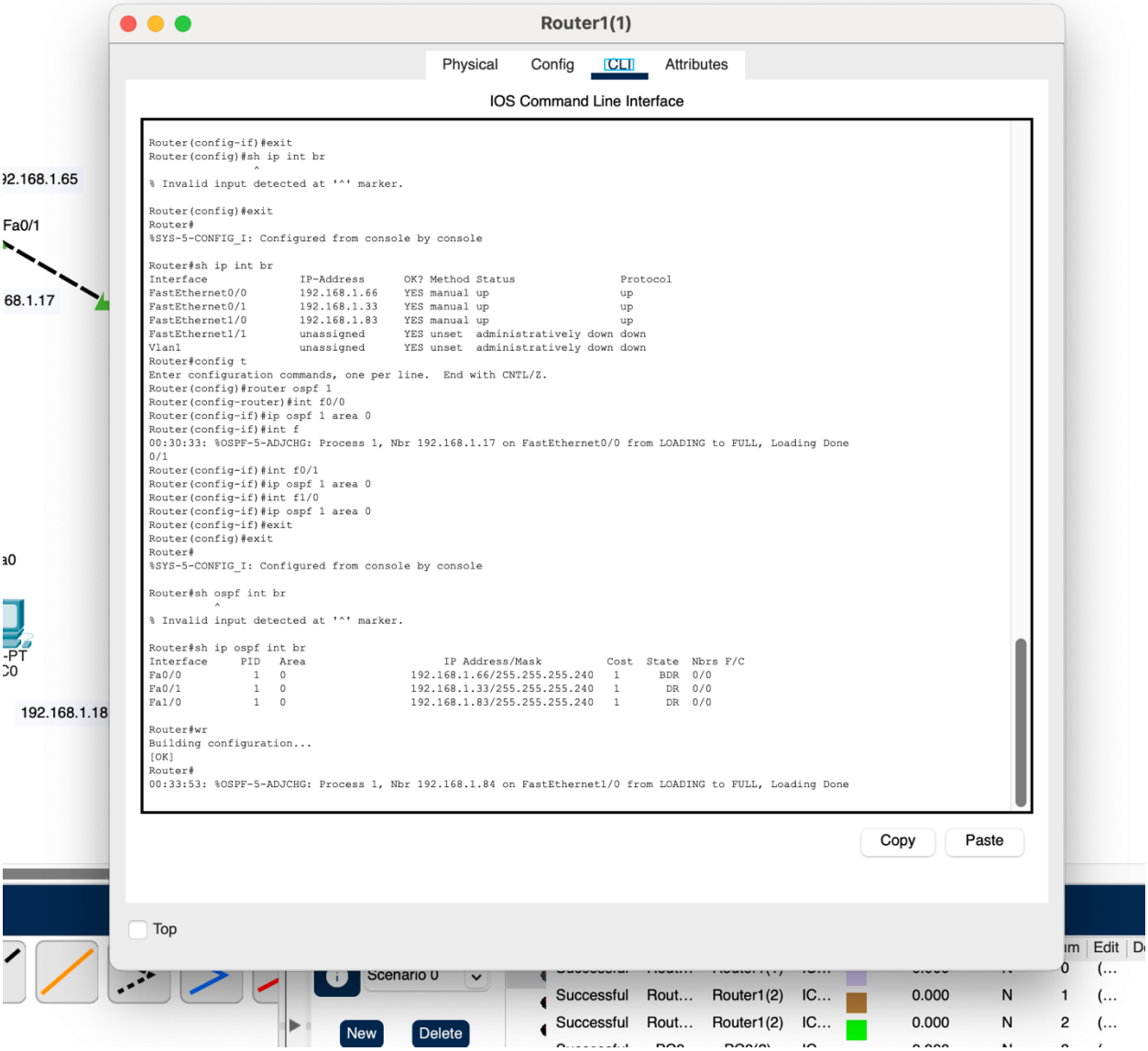
In LAN 07, we are using 192.168.12.32/28 sub-network, the first IP is assigned to Router 192.168.12.33/28 and there are 4 PCs 192.168.12.34/28 - 192.168.12.37/28 will be assigned to PCs.

Dynamic Routing

To ensure efficient and automatic routing between different networks, the OSPF protocol is configured. All routers are placed in OSPF Area 0. The command ip ospf 1 area 0 is applied to all router interfaces to enable OSPF on the network.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC 4.3	PC 2.2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC 8.2	PC 1.5	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC 3.3	PC 8.5	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC 1.3	PC 8.2	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC 2.5	PC 4.3	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC 8.6	PC 3.2	ICMP		0.000	N	5	(edit)	(delete)

As form the above screenshot we can se that we are using ICMP (Internet Control Message Protocol), it is used for diagnostic messages like ping etc. It is using TCP/IP protocol suite for communication between devise.



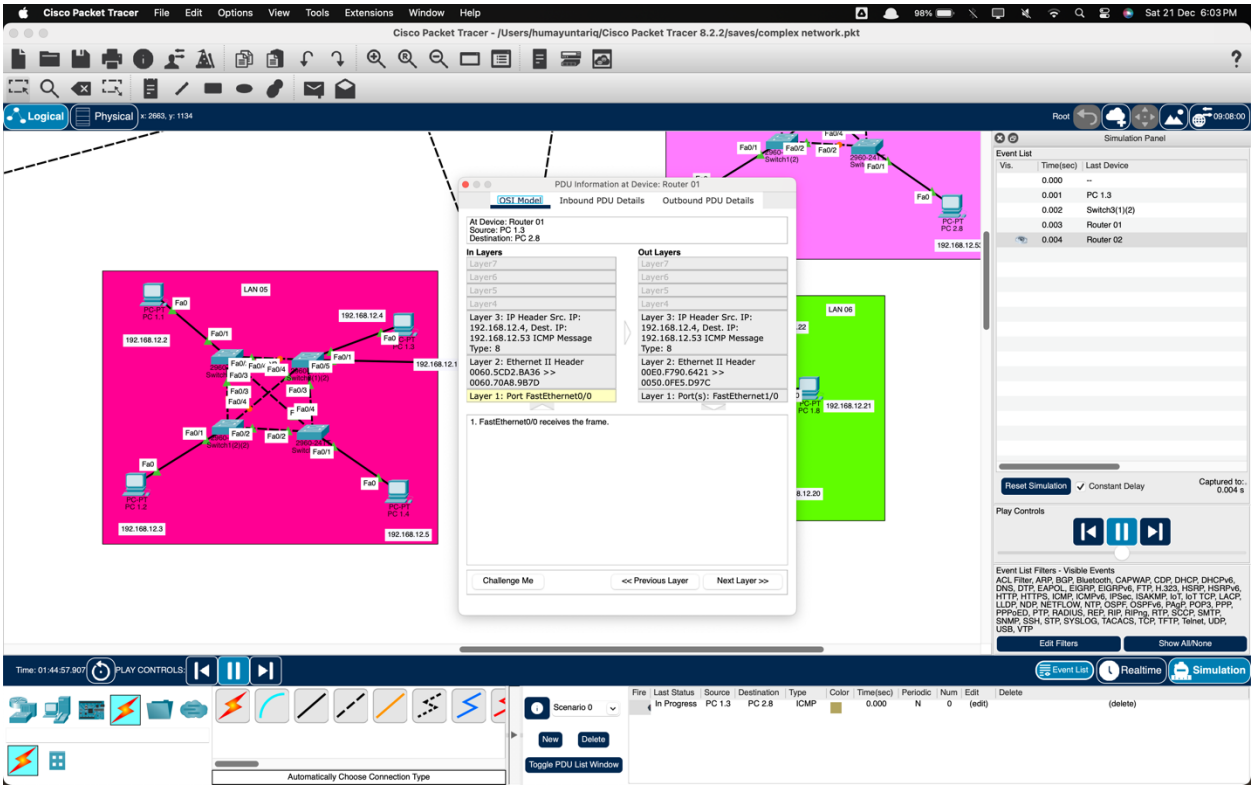
Packet Analysis

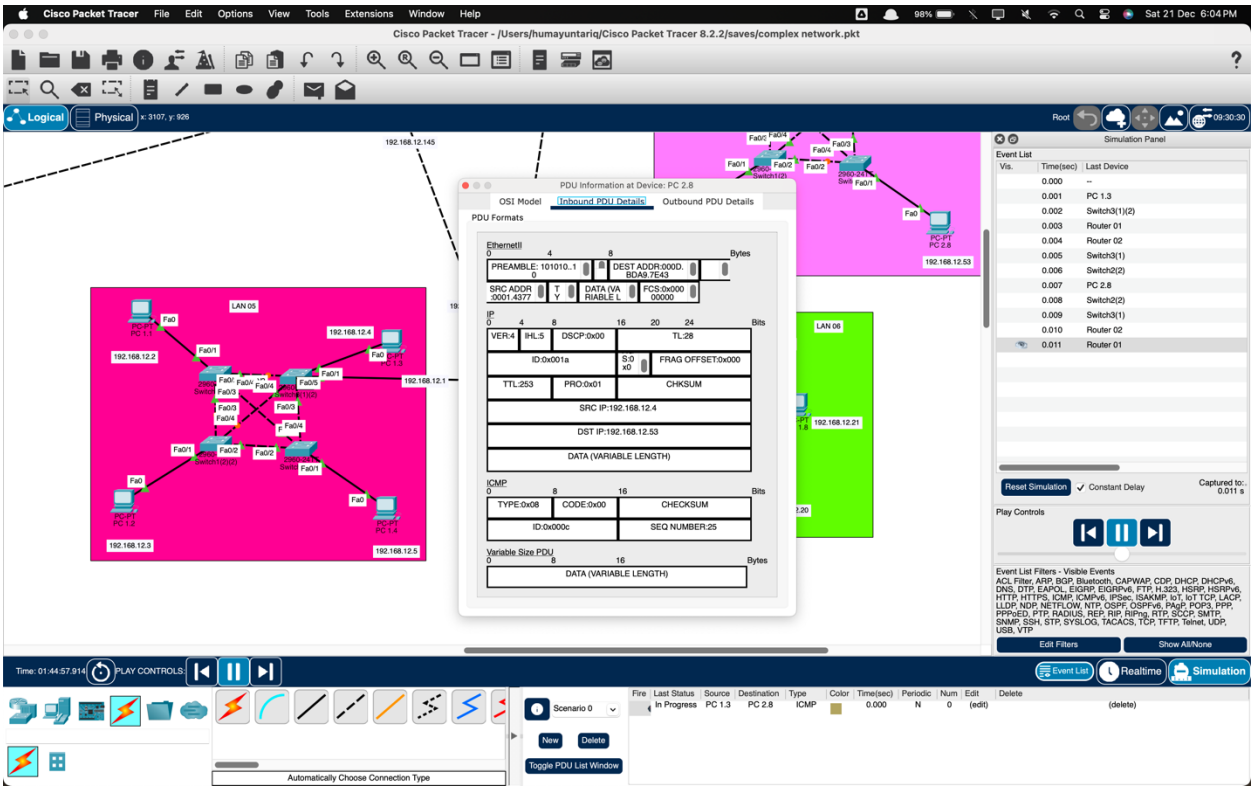
The flow of packets within the network is analyzed using:

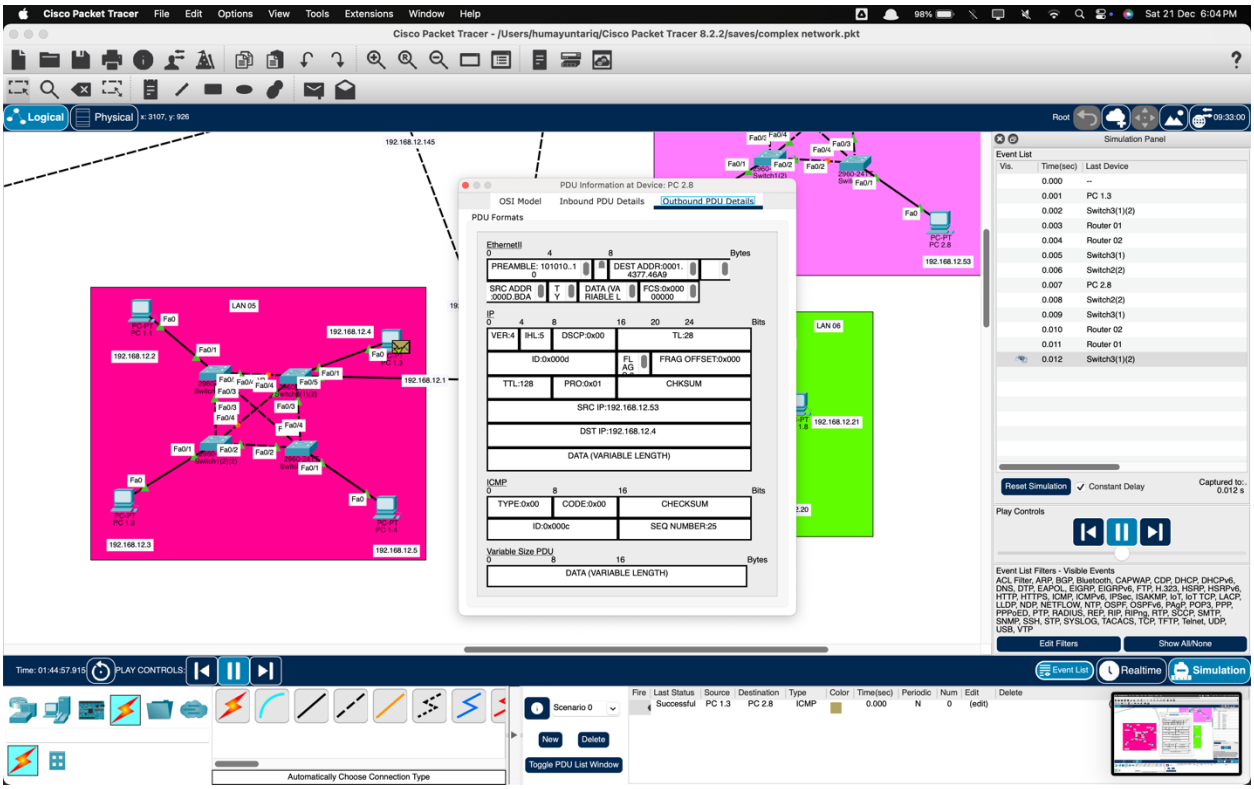
- Wireshark: A tool for capturing and inspecting packets to understand their source, destination, and other details.
- Cisco Packet Tracer: A simulation tool that provides a visual representation of packet flow, enabling easier troubleshooting and validation of network configurations.

In Cisco Packet Tracer

Like **Wireshark** in Cisco Packet Tracer, if we send a packet form one device to another, then in simulation mode we inspect and it shows all sort of data about the packet, like source IP and destination IP, flag, IP version etc.

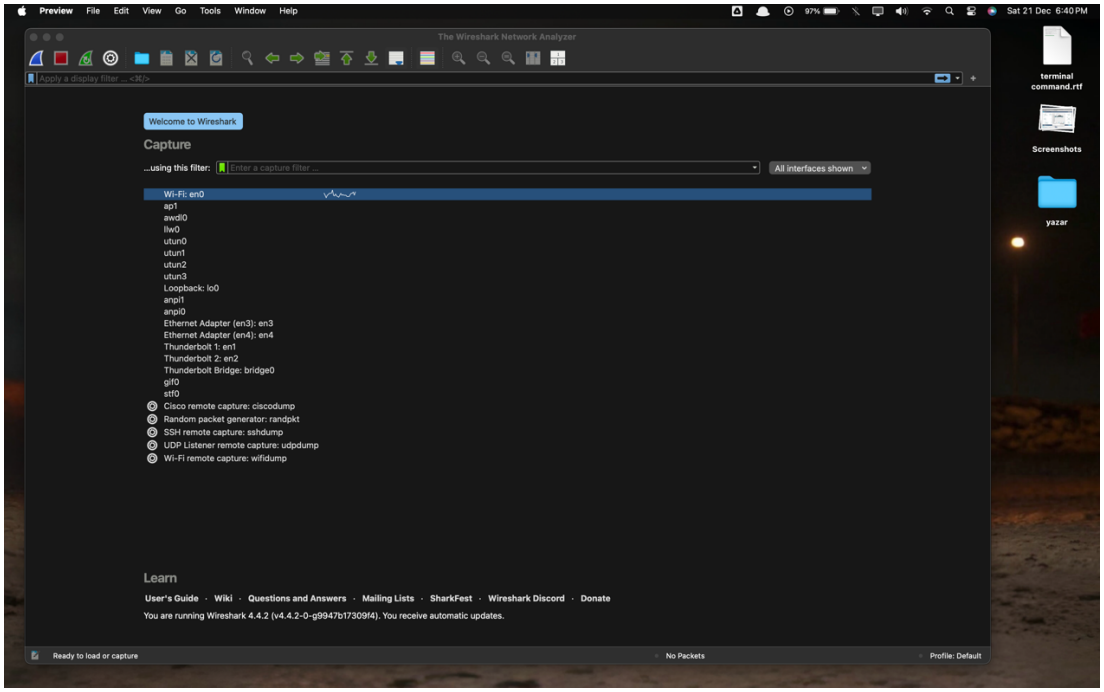

Cisco Packet Tracer File Edit Options View Tools Extensions Window Help
Cisco Packet Tracer - /Users/humayuntariq/Cisco Packet Tracer 8.2.2/saves/complex network.pkt
Logical Physical
PDU Information at Device: Router 01
OSI Model Inbound PDU Details Outbound PDU Details
At Device: Router 01
Source: PC 1.3
Destination: PC 2.8
In Layers
Out Layers
Layer 3: IP Header Src. IP: 192.168.12.4, Dest. IP: 192.168.12.53 ICMP Message Type: 8
Layer 2: Ethernet II Header 0060.5CD2.BA36 >> 0060.70A8.9B7D
Layer 1: Port FastEthernet0/0
Layer 3: IP Header Src. IP: 192.168.12.4, Dest. IP: 192.168.12.53 ICMP Message Type: 8
Layer 2: Ethernet II Header 00E0.F790.6421 >> 0050.0FE5.D97C
Layer 1: Port(s): FastEthernet1/0
1. FastEthernet0/0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>
LAN 05
LAN 06
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Event List Filters - Visible Events
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type

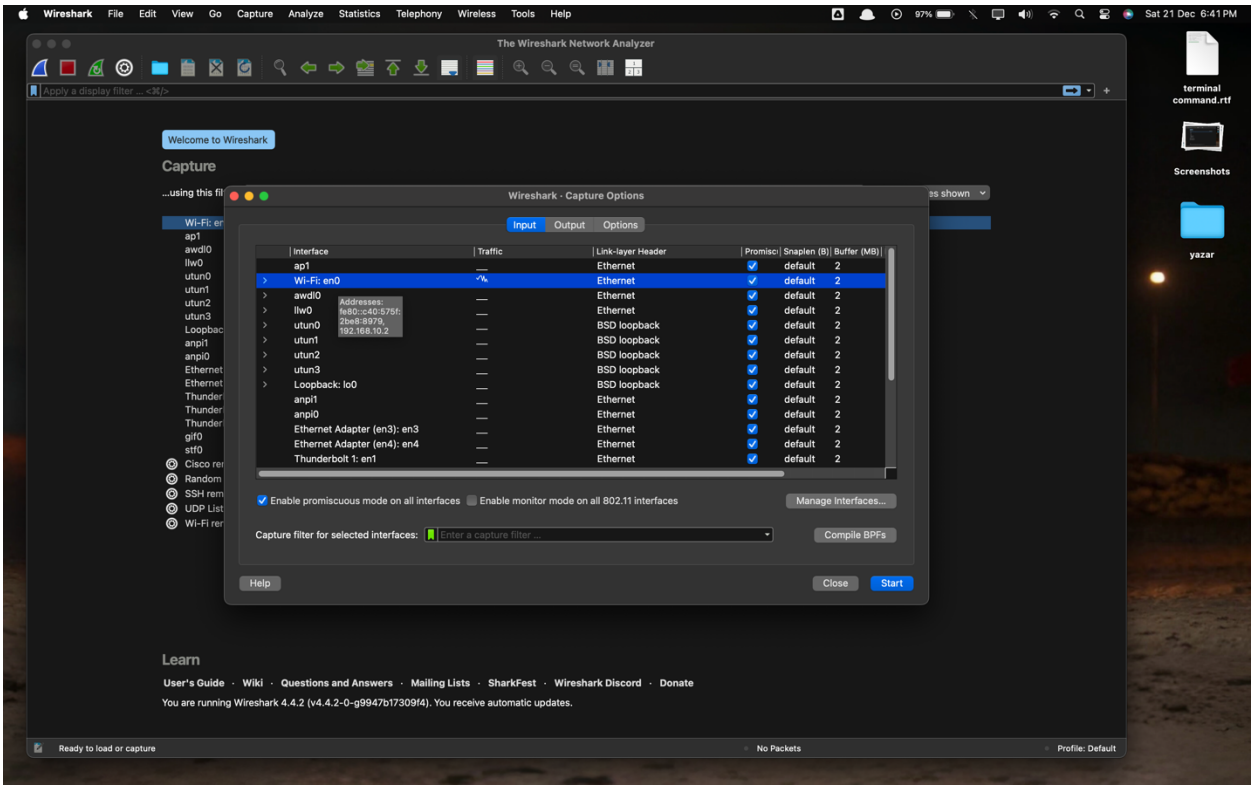

Cisco Packet Tracer File Edit Options View Tools Extensions Window Help
Cisco Packet Tracer - /Users/humayuntariq/Cisco Packet Tracer 8.2.2/saves/complex network.pkt
Logical Physical
PDU Information at Device: PC 2.8
OSI Model Inbound PDU Details Outbound PDU Details
PDU Formats
Ethernet II
IP
ICMP
Variable Size PDU
LAN 05
LAN 06
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Event List Filters - Visible Events
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type



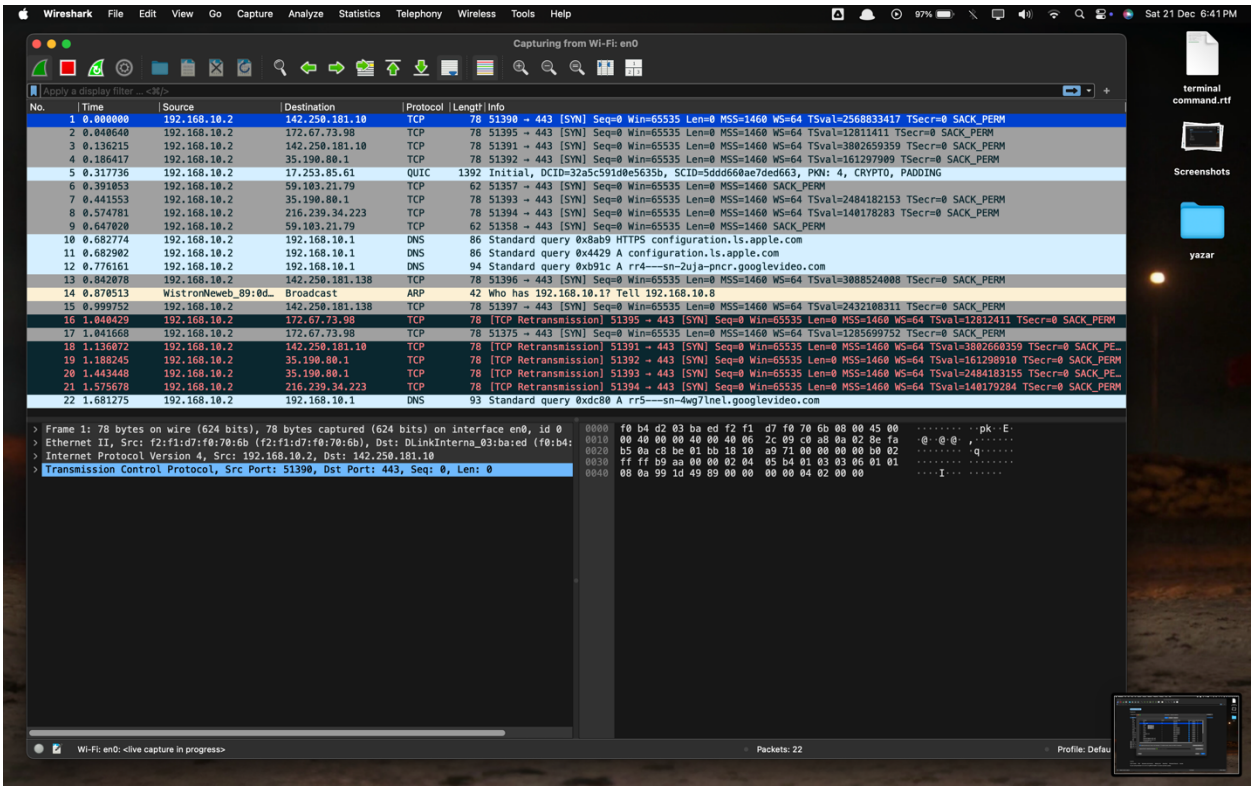
In Wireshark

In Wireshark, after selecting the port we see all the packets that are going through the input that we selected to capture.

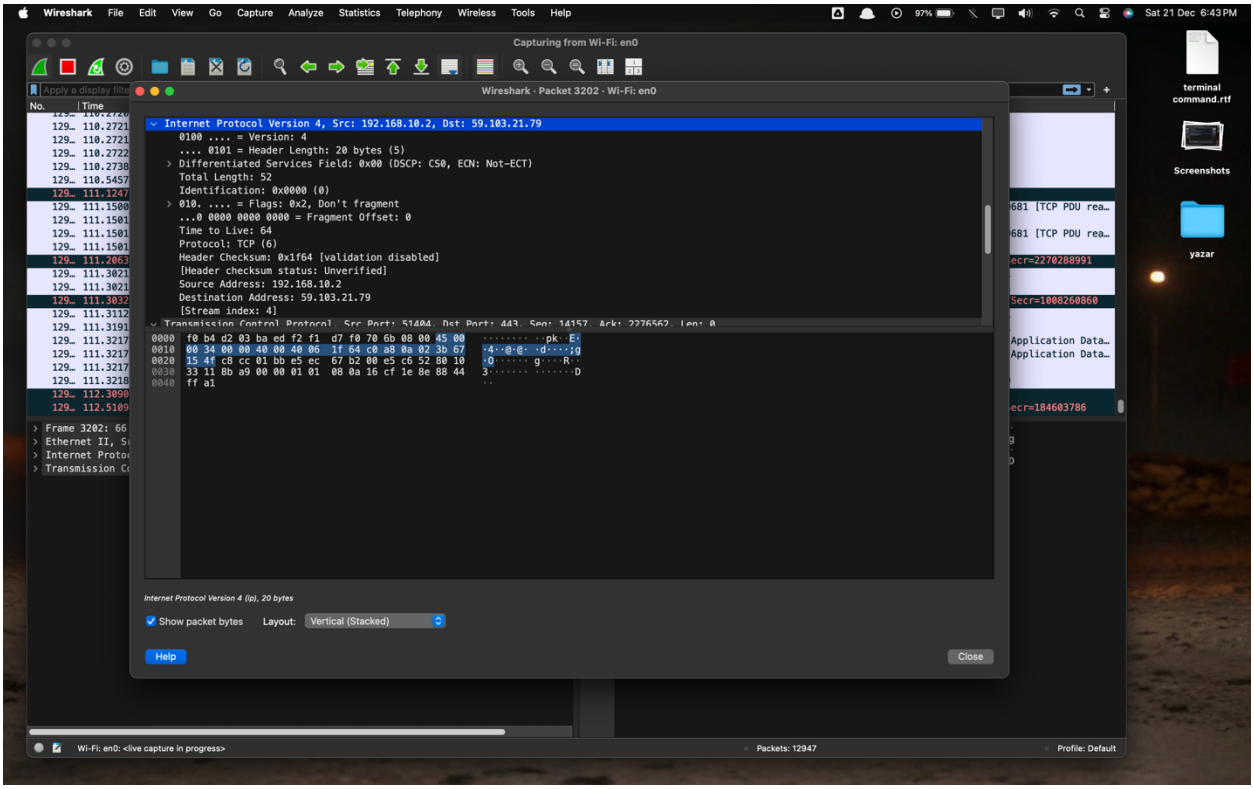




We see all traffic through it, we can selected any packet form this list to capture and see its info.



This show us all the data in the packet like source and destination IP, flag and checksum etc.



Evaluation

The network design was tested by sending data packets between PCs located in different subnets. The following test cases were conducted:

1. Communication from PC 4.3 (LAN 03) to PC 2.2 (LAN 08)
2. Communication from PC 8.2 (LAN 01) to PC 1.5 (LAN 06)
3. Communication from PC 3.3 (LAN 04) to PC 8.5 (LAN 02)

All test cases resulted in successful communication, with packet details verified using Wireshark and Cisco Packet Tracer. The results confirmed that the network was correctly configured and that routing was functioning as intended.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC 4.3	PC 2.2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC 8.2	PC 1.5	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC 3.3	PC 8.5	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC 1.3	PC 8.2	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC 2.5	PC 4.3	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC 8.6	PC 3.2	ICMP		0.000	N	5	(edit)	(delete)

Conclusion

The proposed network design effectively combines multiple topologies to meet the diverse needs of a college environment. Subnetting ensures that IP addresses are managed efficiently, while the OSPF protocol facilitates smooth inter-network communication. Tools such as Wireshark and Cisco Packet Tracer were instrumental in validating the network's functionality. This design provides a scalable, reliable, and cost-effective solution suitable for educational institutions and similar settings.

Reference:

Github: https://github.com/humayyuntariq/Complex-Network-DCN.git

Linkedin: https://www.linkedin.com/posts/humayuntariq_networkingproject-ciscopackettracer-subnetting-activity-7278848048993062913-X-Xt?utm_source=share&utm_medium=member_desktop