|  |  |  |  |
| --- | --- | --- | --- |
| **Lab** | **Title** | **Page no.** | **Remarks** |
| Lab 1 | Introduction to Packet Tracer. | 3 |  |
| Lab 2 | Building a Local Area Network using Packet Tracer. | 4 – 6 |  |
| Lab 3 | Interconnecting two different LANs and testing the connectivity between them. | 7 – 9 |  |
| Lab 4 | DHCP, DNS and Web server configuration using Packet Tracer. | 10 - 15 |  |
| Lab 5 | Implementation of VLANs (Virtual Local Area Network) using Packet Tracer. | 16 – 20 |  |
| Lab 6 | Implementation of OSFP (Open Shortest Path First) using Packet Tracer. | 21- 23 |  |
| Lab 7 | Configure FTP (File Transfer Protocol) using Packet Tracer. | 24-25 |  |
| Lab 8 | Connecting two PCs with RJ45 cable(Ethernet cable) | 26-30 |  |
| Lab 10 | Introduction to Wire-Shark | 31-33 |  |
| Lab 11 | HTTP Protocol Analysis Using Wire-shark | 34-35 |  |
| Lab 12 | Using all the Filters in WireShark | 36-39 |  |

**TABLE OF CONTENTS**

**LAB 1**

**TITLE:** INTRODUCTION TO PACKET TRACER.

**BACKGROUND THERORY:**

Cisco Packet tracer is a network simulation tool developed by Cisco. It allows users to create, configure, and test virtual network topologies without needing physical devices. It is widely used by students to learn about networking concepts, routing, switching, VLANs and more. The software provides a drag-and-drop interface for routers, switches, PCs, and cables, making it easy to build and simulate networks. The interface if Cisco packet Tracer is shown below in figure.

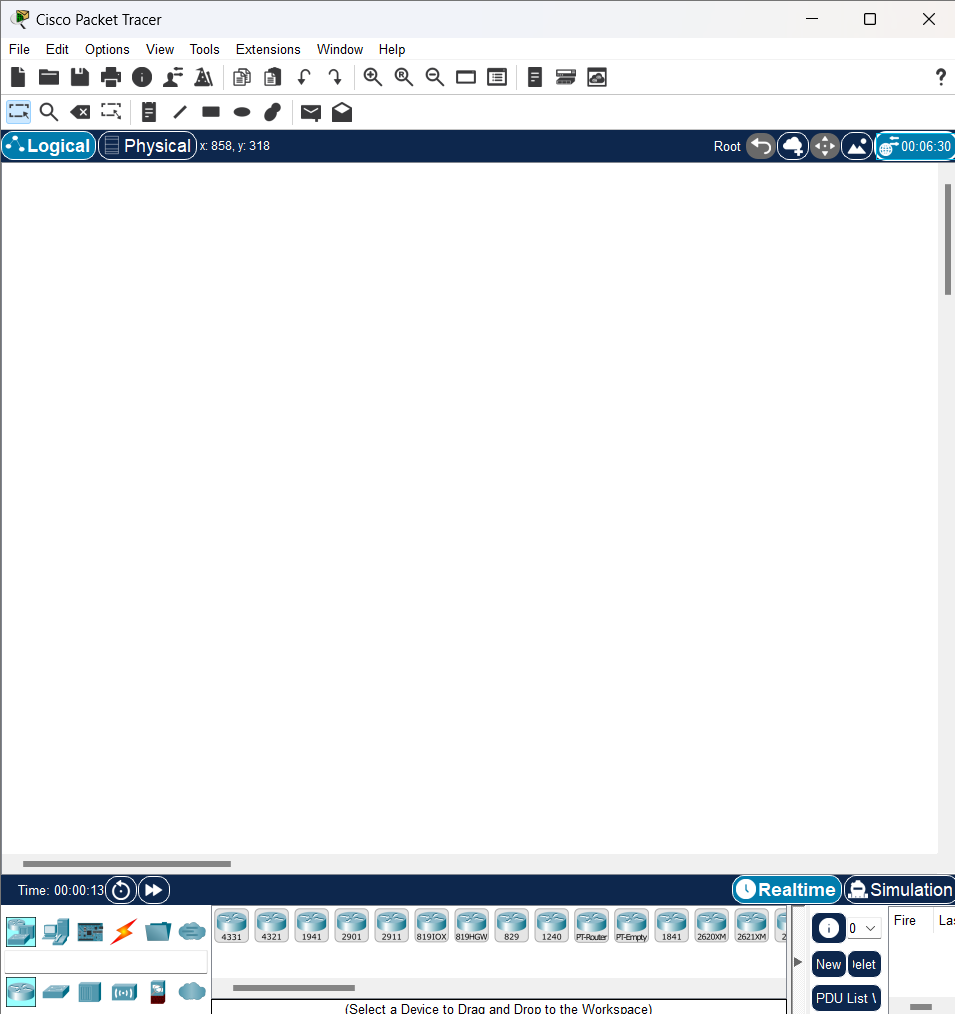


Figure 1: Interface of Cisco Packet Tracer

**CONCLUSION:**

The aim of this lab is to become familiar with Cisco Packet Tracer. We will learn more about its working environment in the following labs.

**LAB 2**

**TITLE:** BUILDING A LOCAL AREA NETWORK USING PACKET TRACER.

**BACKGROUND THEORY:**

A LAN is a group of computers/devices connected in a small area like an office, school, or home. All devices can share resources (files, printers, Internet) and communicate with each other. LANs use switches to connect multiple devices.

**NETWORK DEVICES REQUIRED:**

* A switch
* 2 PCs
* 2 laptops
* Straight through wires

**PROCESS:**

Step 1: Set up the devices.

* Add 1 2960 switch
* Add 2 PCs (PC0,PC1)
* Add 2 laptops (laptop0, laptop1)
* Connect all the devices to switch.

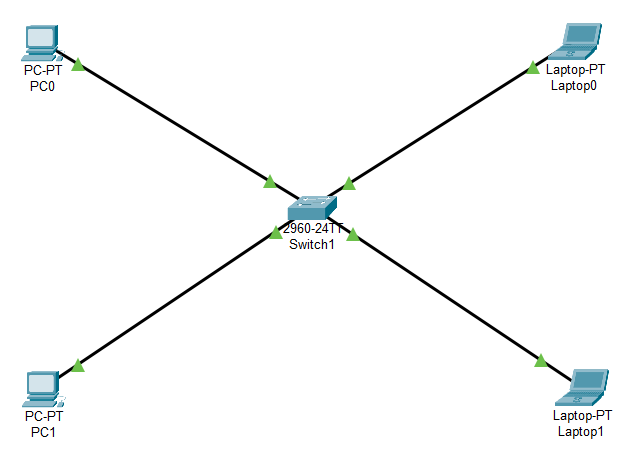
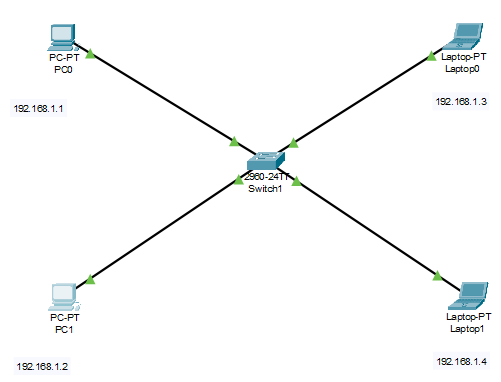


Figure 2: Connection between devices and switch

Step 2: Assign IP addresses to PCs and laptops.

Click each PC→ Desktop →**IP Configuration**

****

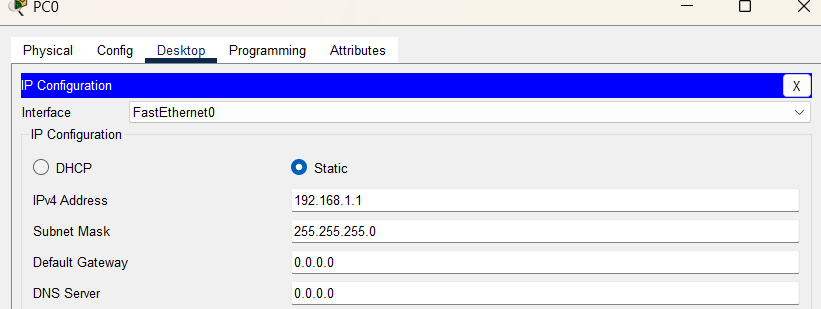
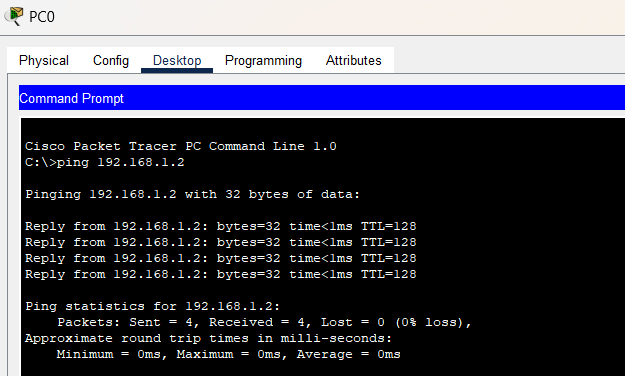


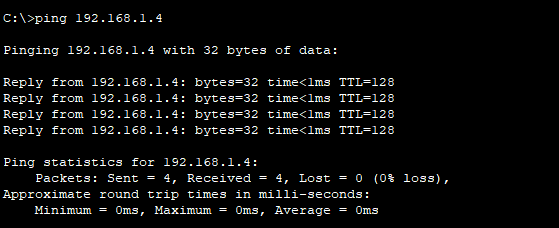
Figure 3: Assigning IP address to PC0

Step 3: Checking the connection between PCs and laptops to make sure they can send/receive packets.

* First from PC0 to PC1. Ping IP address of PC1 on PC0.
* On PC0, go to Desktop -> Command prompt



* Secondly, laptop0 to laptop1.



**OBSERVATION:**

All the devices are connection to each other and can send/ receive packets.

**CONCLUSION:**

Simple LAN is created using Cisco Packet Tracer.

**LAB 3**

**TITLE:** INTERCONNECTION TWO DIFFERENT LANS AND TESTING THE CONNECTIVITY BETWEEN THEM.

**BACKGROUND THEORY:**

LAN interconnection or internetworking is the process of interconnection two different LANs using router. In this lab two different LANs are used to test the connectivity between them. LANs are commonly used in home WIFI networks and small business networks.

**NETWORK DEVICES REQUIRED:**

* Router
* 2 Switches
* 4 PCs
* Straight through wires

**PROCESS:**

Step 1: Set up all the devices and establish the connection between them using wires.

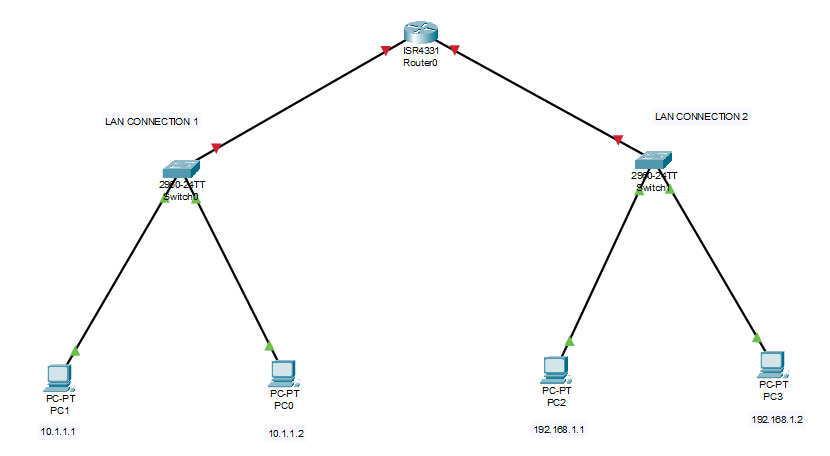


Figure 4: Connecting devices using wires

Step 2: Assign IP addresses to all the PCs.

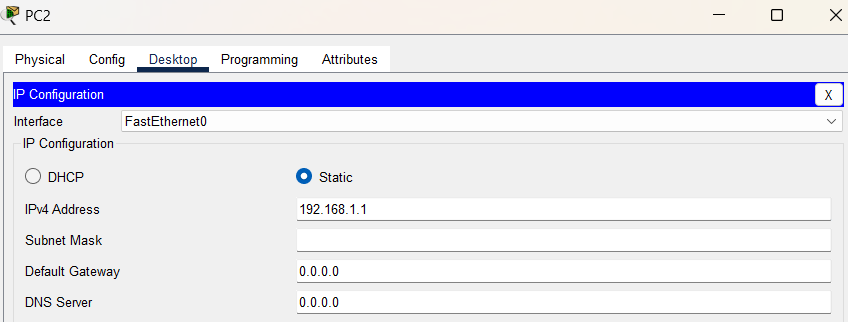
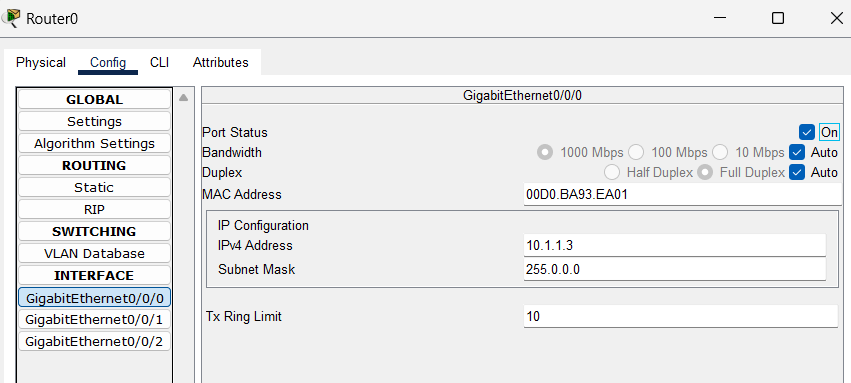


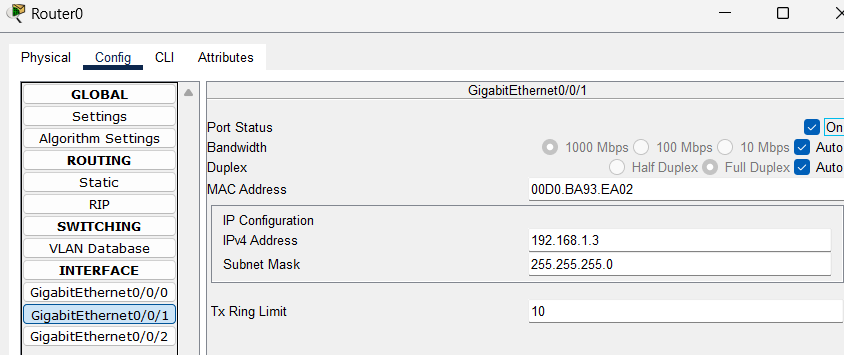
Figure 5: Assigning IP address to PC2

Step 3: Enabling the connection with router.

* Click on router -> Config ->GigabitEthernet0/0/0 and assign the IP address.

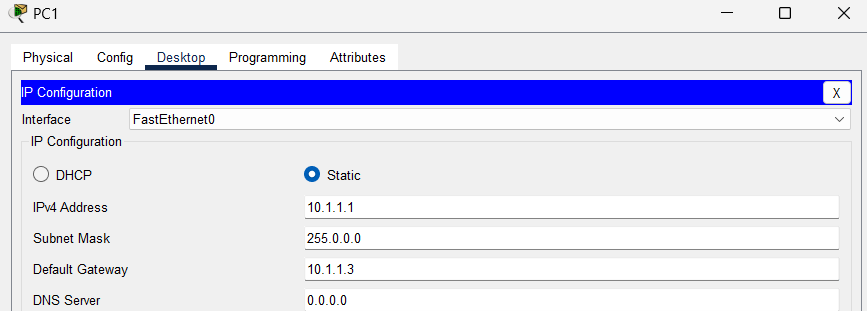


* Click on router -> Config ->GigabitEthernet0/0/1 and assign the IP address.

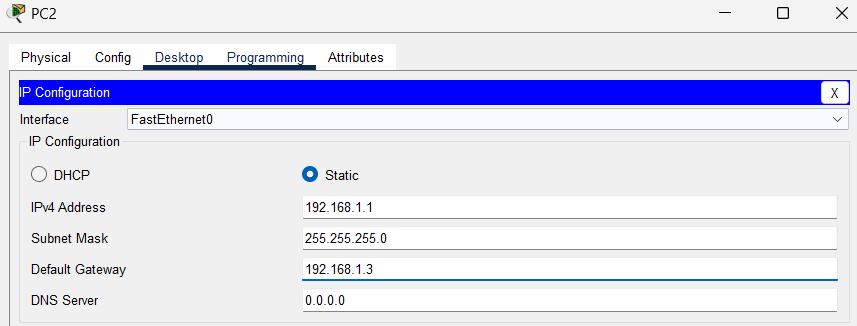


Step 4: Assign Default Gateway to LAN CONNECTION 1 AND 2 PCs.

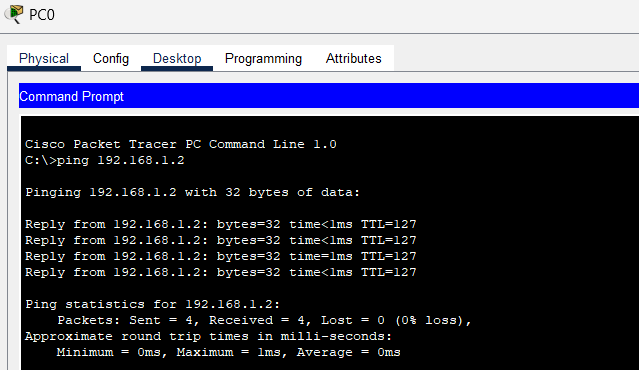
* For PC1 of LAN1, click on PC1 -> desktop -> IP configuration -> default Gateway.



* Similarly, for PC0 assign the same value.
* Again, for PC2 of LAN2,



Step 5: Check the connectivity for PC0 TO PC4.



**CONCLUSION:**

The two different LAN CONNECTIONs are interconnected with each other.

**LAB 4**

**TITLE:** DHCP, DNS AND WEB SERVER USING PACKET TRACER.

**BACKGROUND THEORY:**

In a network, DHCP, DNS, Web server work together to provide essential services.

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices, making network setup easier.

DNS (Domain Name System) translated domain name (like [www.google.com](http://www.google.com)) into IP addresses so browsers can locate websites.

A Web Server hosts websites and delivers web pages to users over the internet or local network.

**NETWORK DEVICES REQUIRED:**

* A router
* A switch
* 3 servers
* 3 PCs
* 1 laptop
* Cables

**PROCESS:**

Step 1: Set up all the devices.

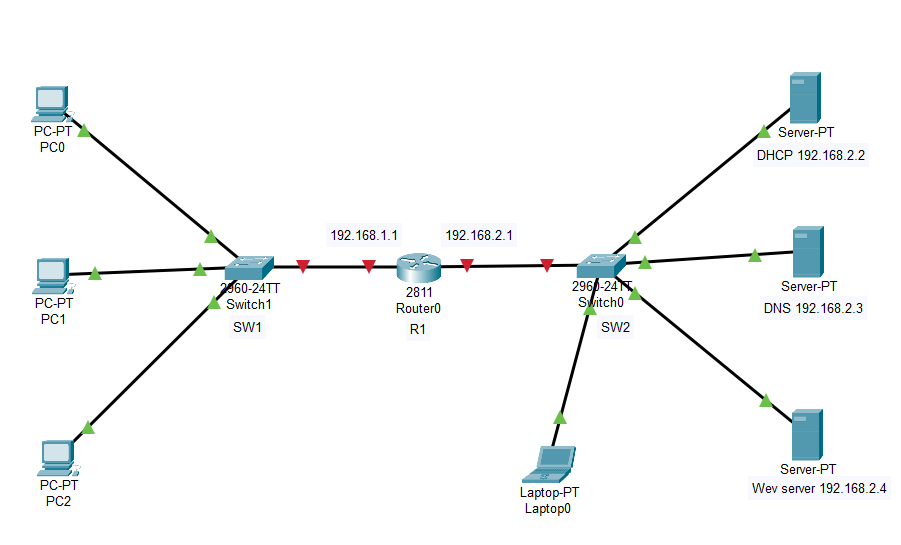
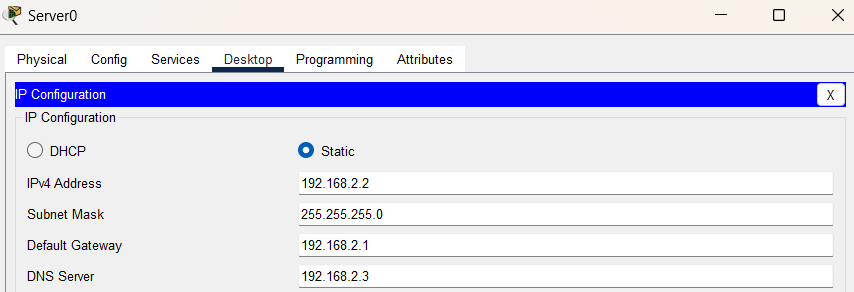


Figure 6: Connecting all the devices using cables

Step 2: Assign IP address to DHCP server.

Click on server→ Desktop →**IP Configuration**

****

**Step 3: Enable the service for DHCP and create two pools: serverPool0 and serverPool1.**

Click on server→ services →**DHCP**

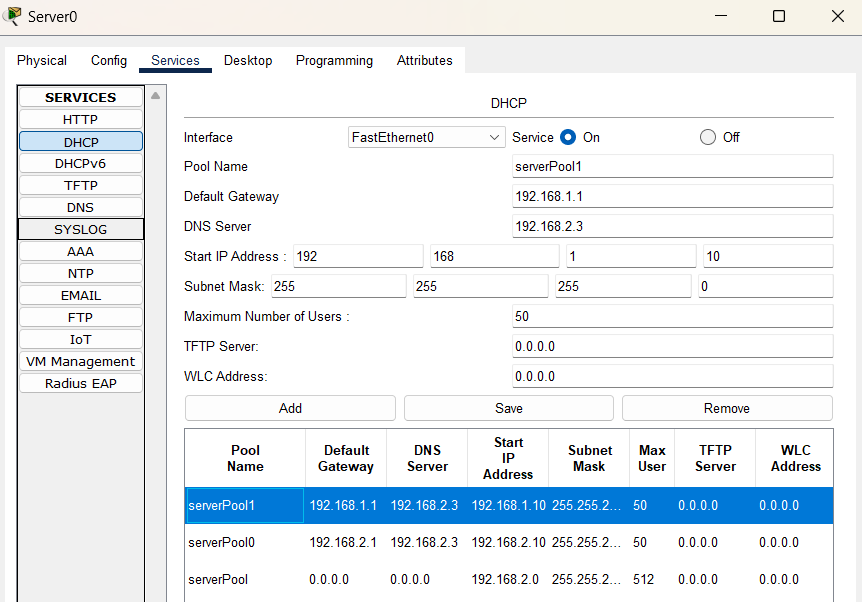
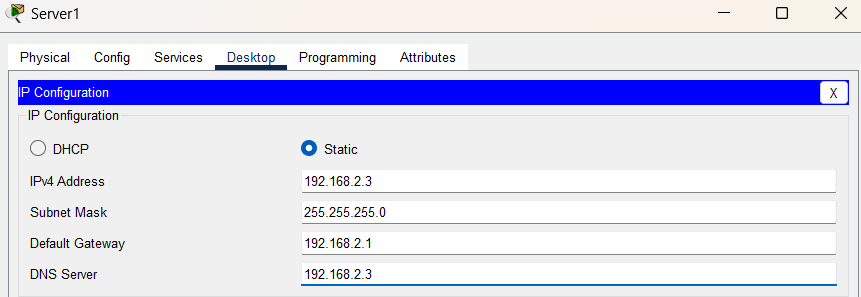
****

Figure 7: Configuration of DHCP server

**Step 4: Assign IP address to DNS server.**

****

**Step 5: Give Domain name to your server.**

Click on server→ services →**DNS**

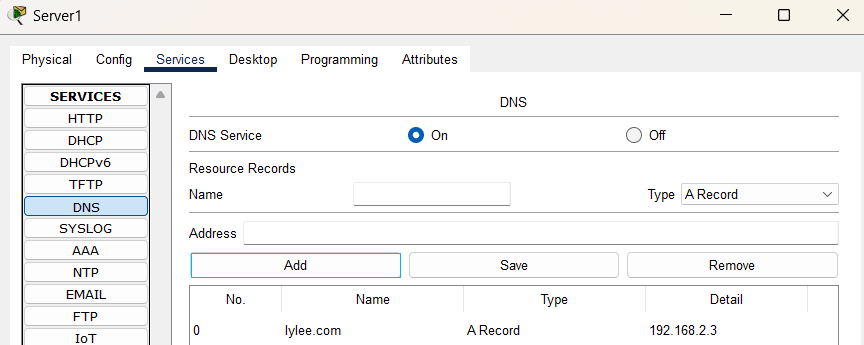
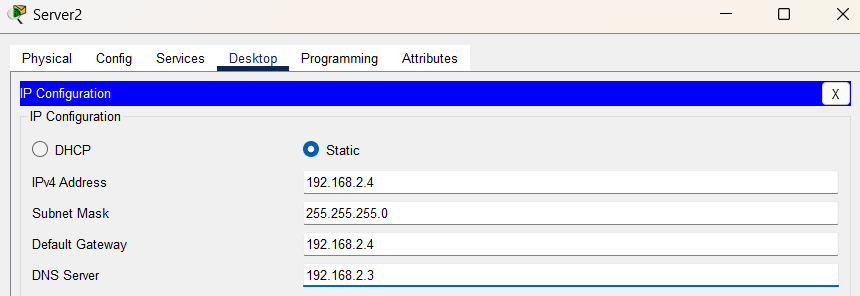
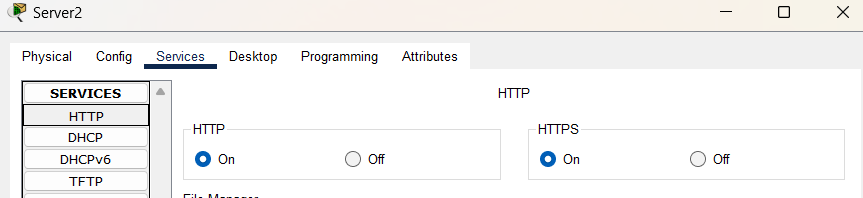
****

Figure 8: Configure DNS server

**Step 6: Assign IP address to Web server.**

****

**Step 7: Enable http services.**

****

**Step 8: Check DHCP server configuration.**

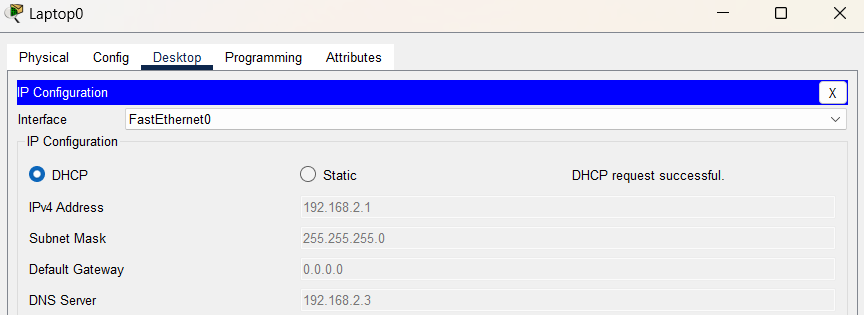
****

Figure 9: Successful DHCP configuration

Step 9: Check DNS and web server.

Click on server→ Desktop →**Web browser**

****

Figure 10: DNS and web browser

Step 10: Configure the router.

Click on router→ CLI

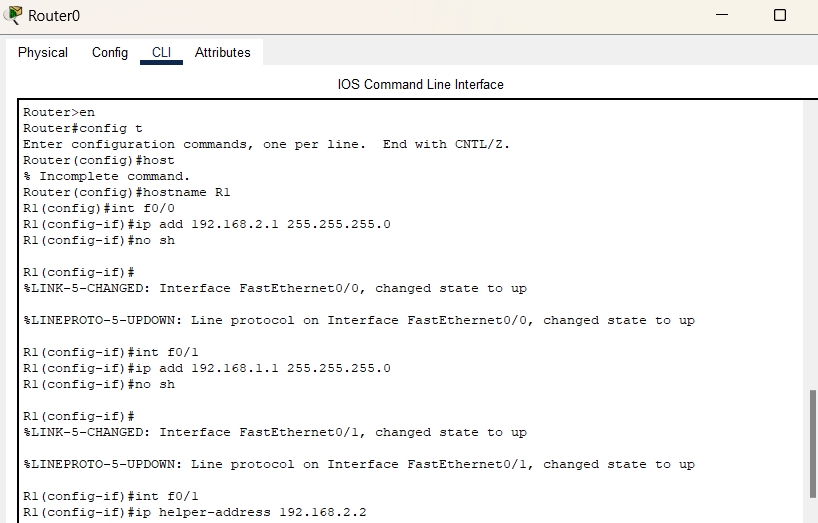


Figure 11: Configuration of router

Step 11: Check DHCP connection with PC0

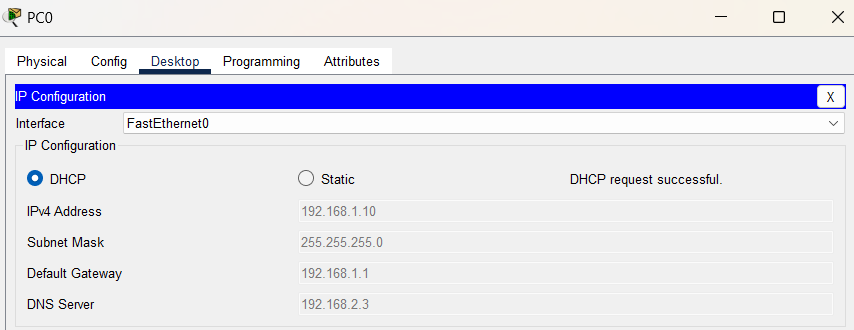
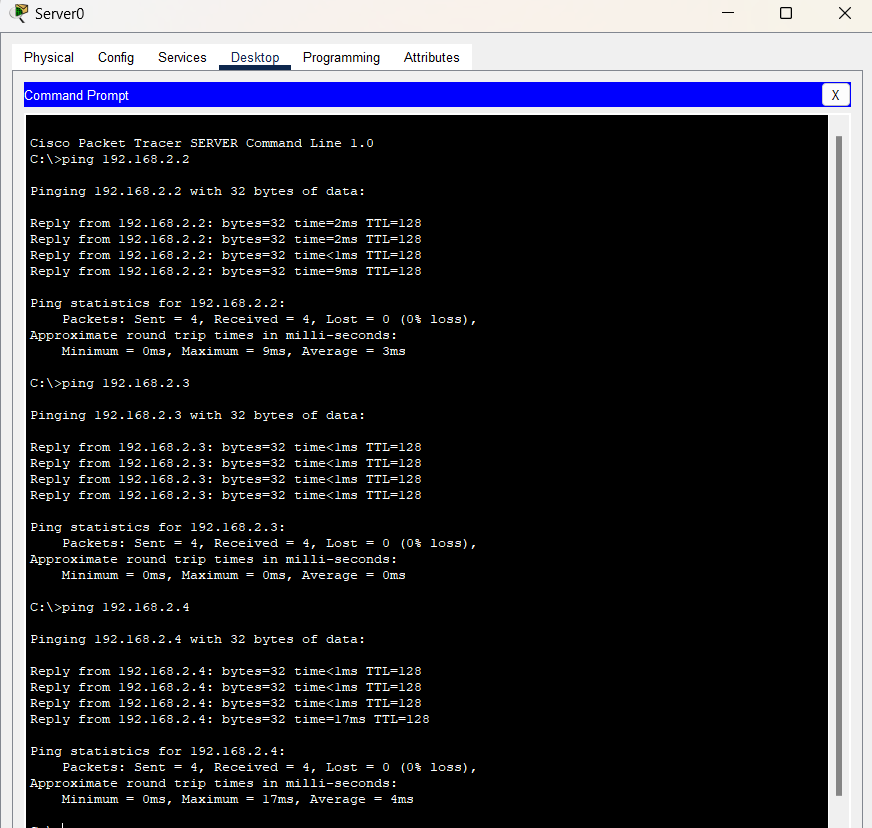


Figure 12: Successful DHCP connection with PC0

**OUTPUT:**

****

**CONCLUSION:**

DHCP, DNS and web server is successfully configured using packet tracer.

**LAB 5**

**TITLE:** IMPLEMENTATION OF VLAN USING PACKET TRACER

**BACKGROUND THEORY:**

VLAN (Virtual LAN) divides a physical LAN into multiple logical networks. Devices in the same VLAN can communicate even if they are on different switches. VLAN improves network security, reduces broadcast traffic, and allows logical grouping.

Examples:

* VLAN 10 - for admin
* VLAN 20 - for students

**NETWORK DEVICES REQUIRED:**

* 1 switch
* 4 PCs
* Straight- through cables

**PROCESS:**

Step 1: Set up the devices.

* Add 1 2960 switch
* Add 4 PCs (PC0,PC1,PC2,PC3)
* Connect all the PCs to switch.

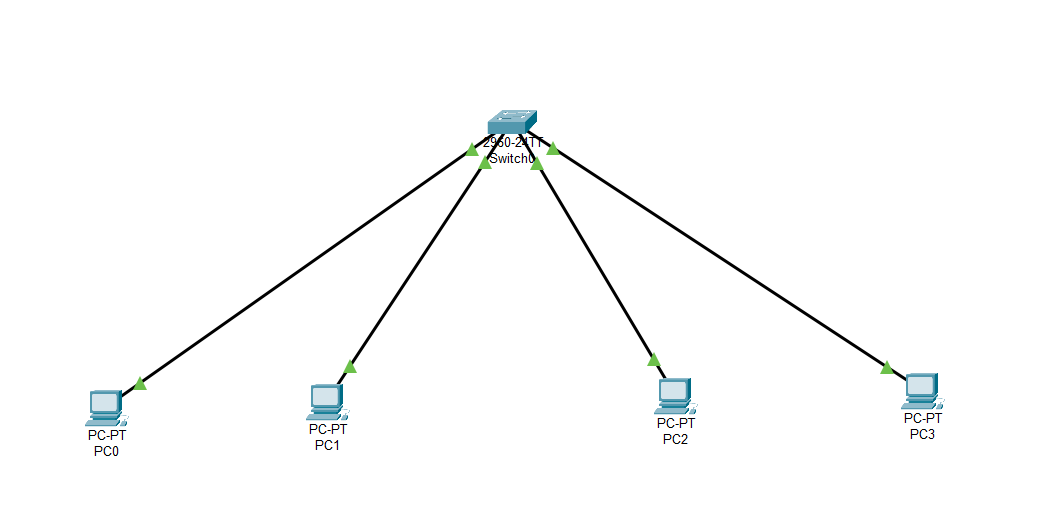
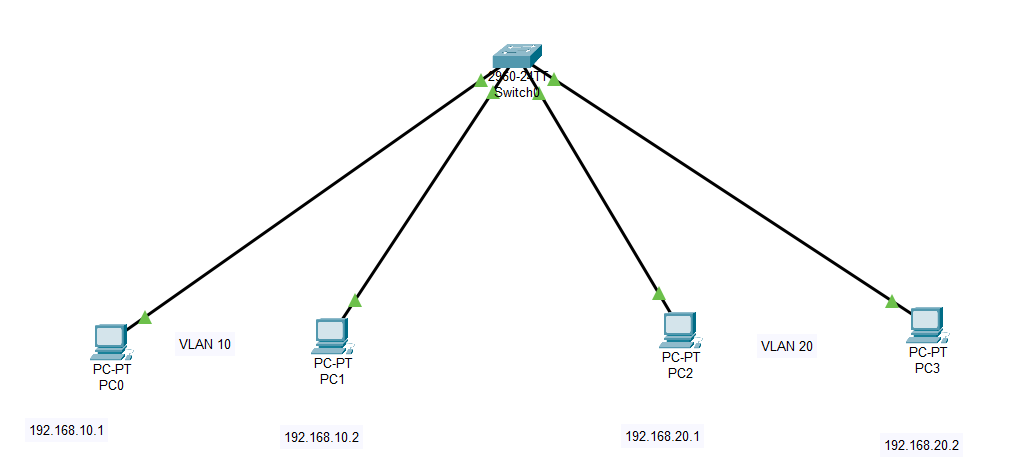
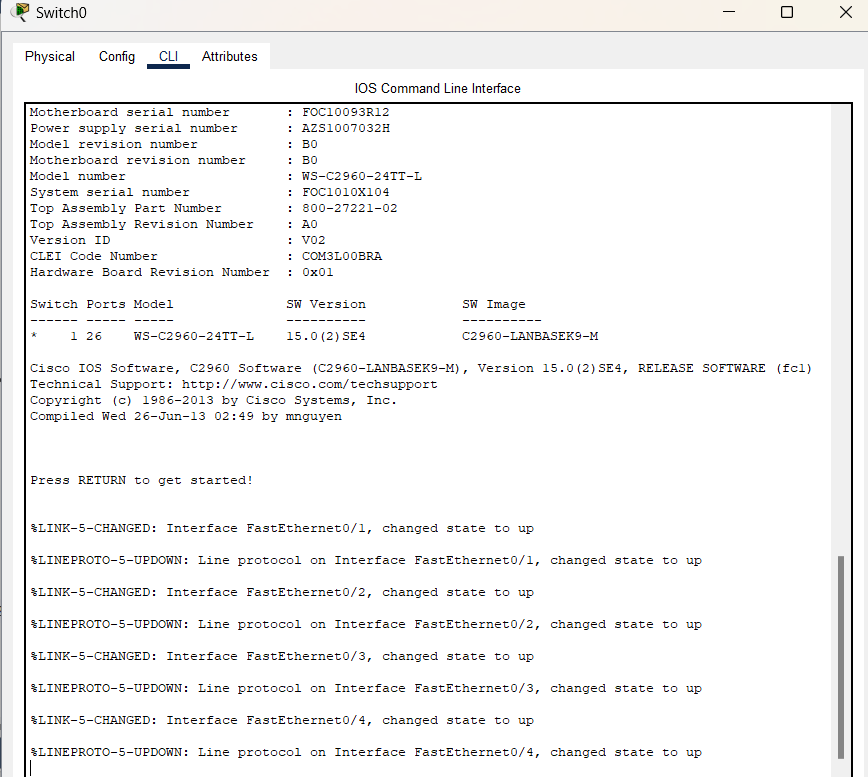


Figure 13: Connection between all the devices using wires

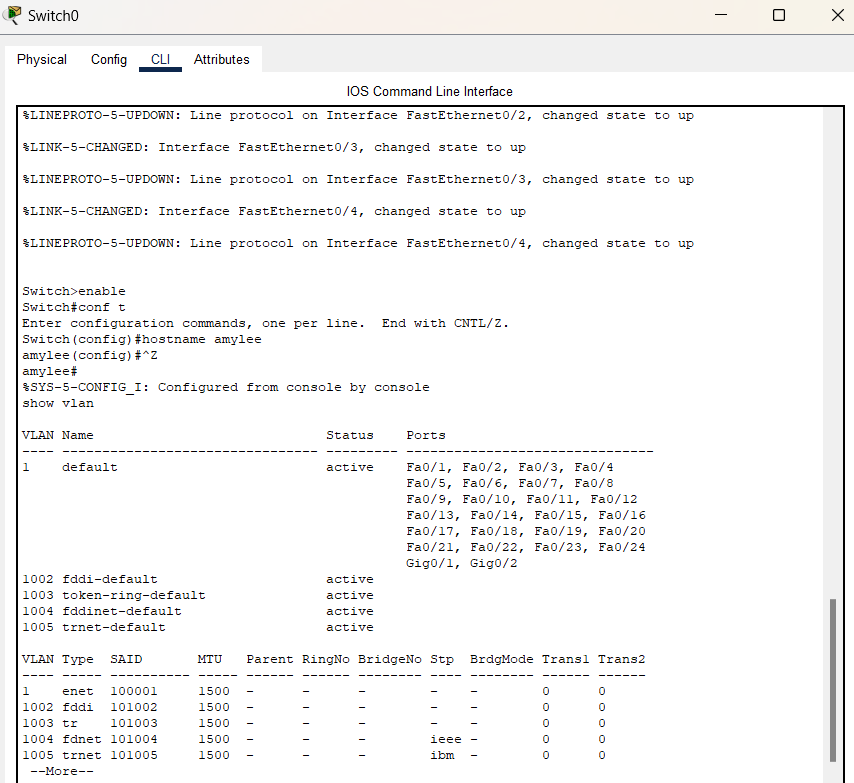
Step 2: Assign IP addresses



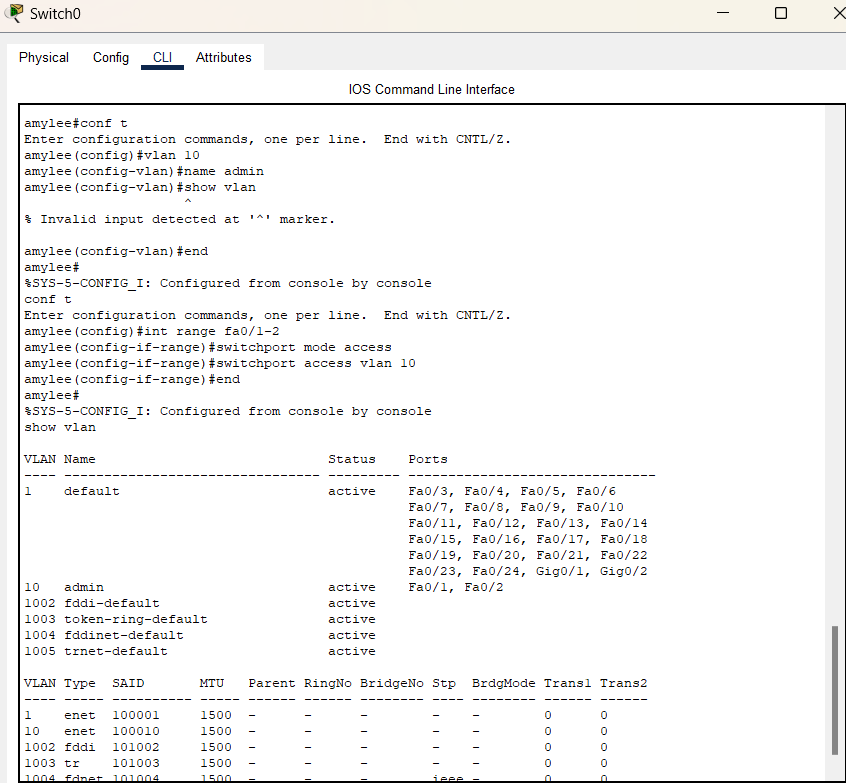
Step 3: Click the switch and go to CLI for configuration.



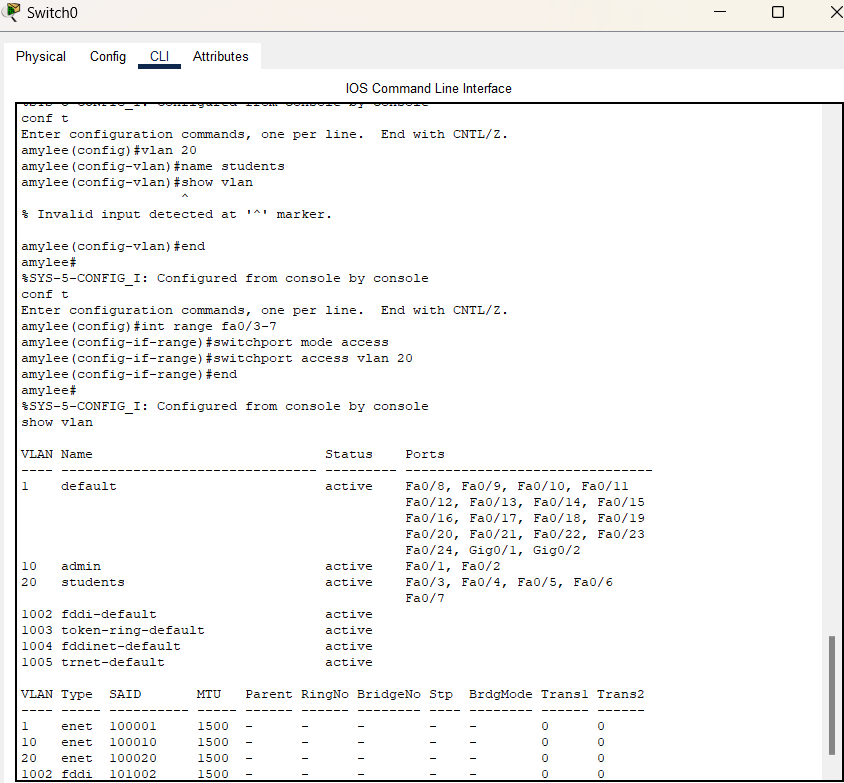
Step 4: Configure VLANs on the switch.



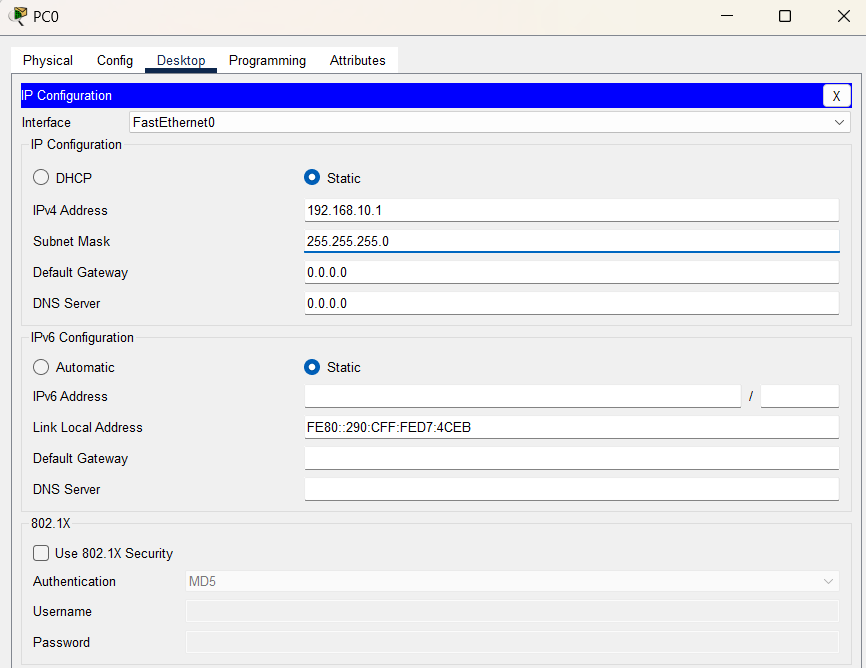
Step 5: Initialize the range of VLAN 10 named admin.



Step 6: Initialize the range of VLAN 20 named students.

****

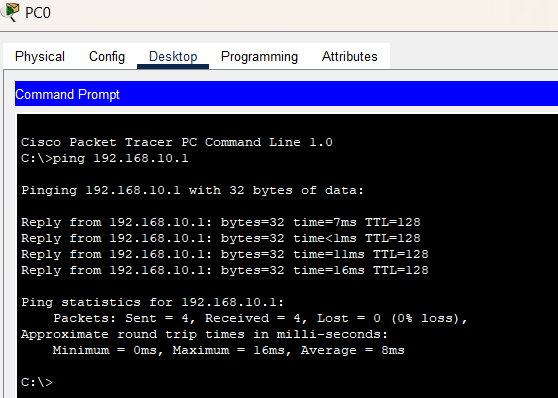
Step 7: Assign IP addresses to all the PCs. Click to pc –>desktop –> IP configuration.



**OBSERVATION:**

Ports fa0/1 and fa0/2 comes under VLAN 10 and fa0/3-7 comes under VLAN 20.

**OUTPUT:**

****

**CONCLUSION:**

VLAN is implemented using Cisco Packet tracer.

**LAB 6**

**TITLE:** IMPLEMENTATION OF OSFP USING PACKET TRACER.

**BACKGROUND THEORY:** OSPF (Open Shortest Path First) is a dynamic routing protocol used to find the best path between routers. It is link-state, supports VLSM and updates only when changes occur. OSPF uses areas (default are is area 0) and identifies routers using Router IDs.

**NETWORK DEVICES REQUIRED:**

* 2 Routers
* 4 PCs
* 2 Switches
* Straight through cables
* Cross-over wire

**PROCESS:**

Step 1: Setup all the devices as in the figure.

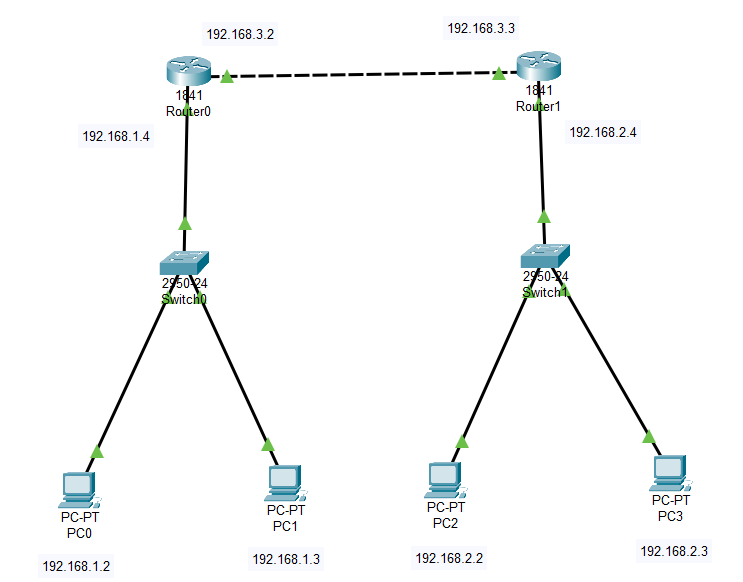


Figure 14: Network devices setup for OSPF

Step 2: Assign IP address to all the PCs like the figure below for PC0.

Click on PC→ Desktop →**IP Configuration**

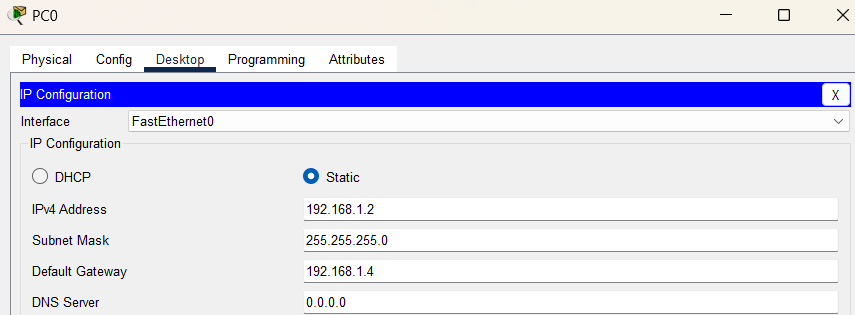
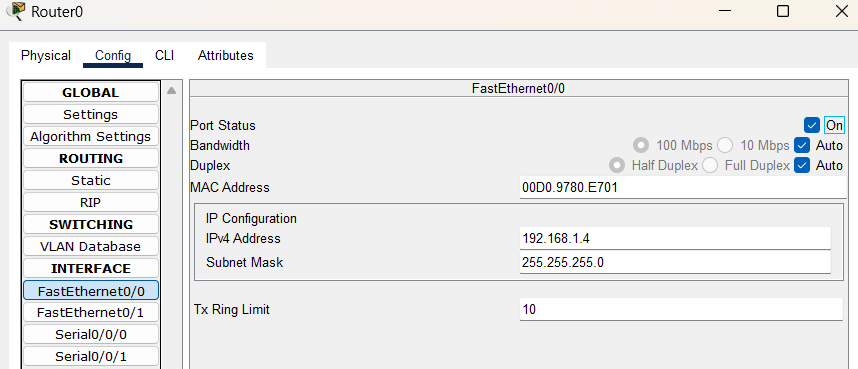
****

Figure 15: Assigning IP address for PC0

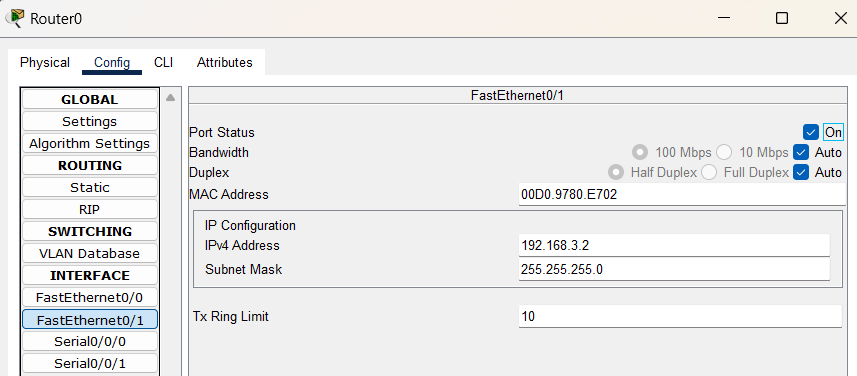
Step 2: Configure Router0

* For FastEthernet0/0,

Click on Router→ Config→FastEthernet0/0



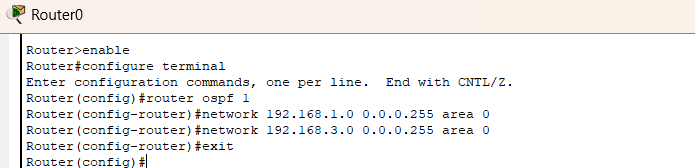
* Again, for FastEthernet0/1



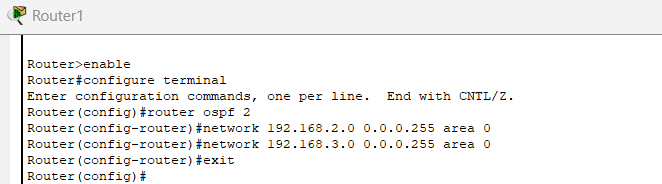
* Configure Router1 assigning 192.168.2.4 IP address for 0/0 and 192.168.3.3 IP address for 0/1.

Step 3: Now, configure OSPF on routers.

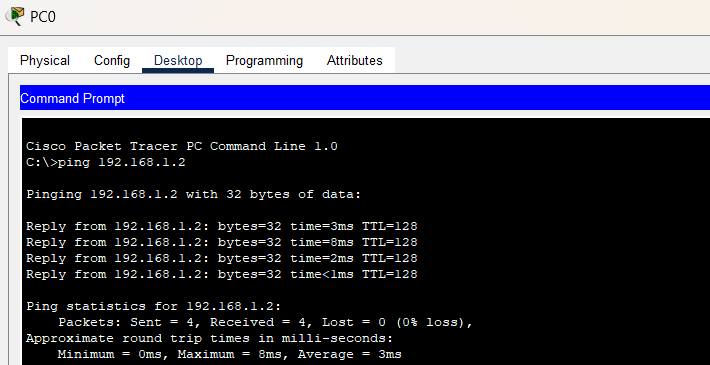
* Router0: Click on Router→ CLI



* Router1:



Step 4: Test the network.



**CONCLUSION:**

OSFP is implemented successfully using Cisco Packet tracer

**LAB 7**

**TITLE:** CONFIGURE FTP SERVER USING CISCO PACKET TRACER.

**BACKGROUND THEORY:**

The primary purpose of an FTP server is to allow users to upload and download files. An FTP server is a computer that has a file transfer protocol (FTP) address and is dedicated to receiving an FTP connection. FTP is a protocol used to transfer files via the internet between server (sender) and a client (receiver). An FTP server is a computer that offers files available for download via an FTP protocol, and it is common solution used to facilitate remote data sharing between computers.

**NETWORK DEVICES REQUIRED:**

* 1 server
* 1 switch
* 2 PCs
* Straight through wires

**PROCESS:**

Step 1: Connect PCs and server to the switch using straight through cables.

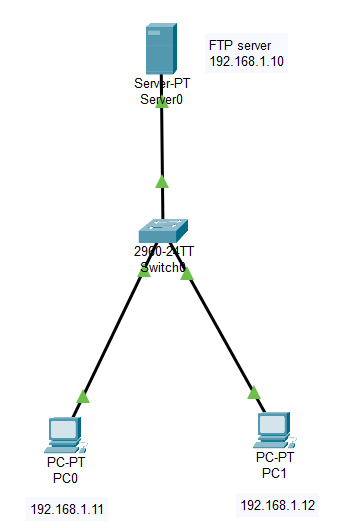
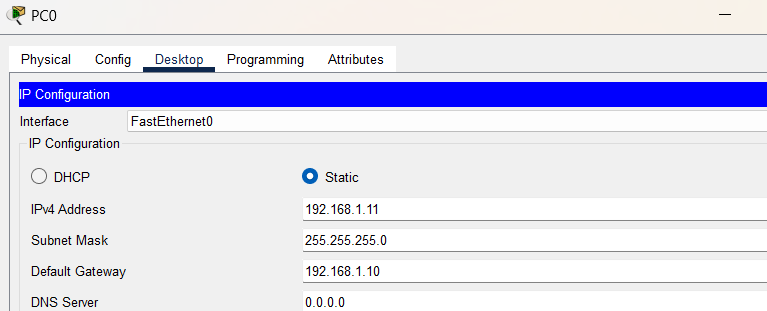


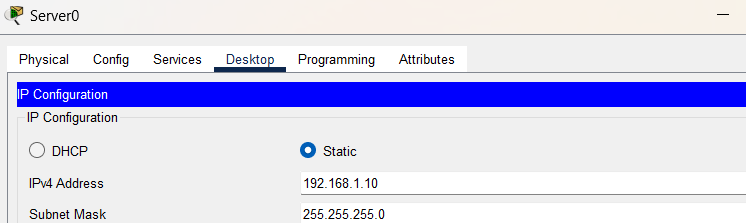
Figure 16: FTP server configuration

Step 2: Assign IP addresses to PCs and server.

* For each PC, → Desktop → IP Configuration

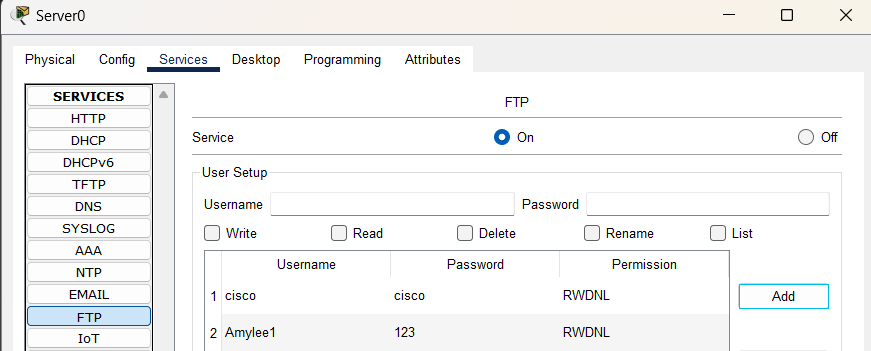


* Assign 192.168.1.12 to PC1.
* Now, for server:



Step 3: Configure the FTP server.

Server → Services → FTP, add username and password.



Step 4: Test FTP from PC0

PC0 → Desktop → Command Prompt

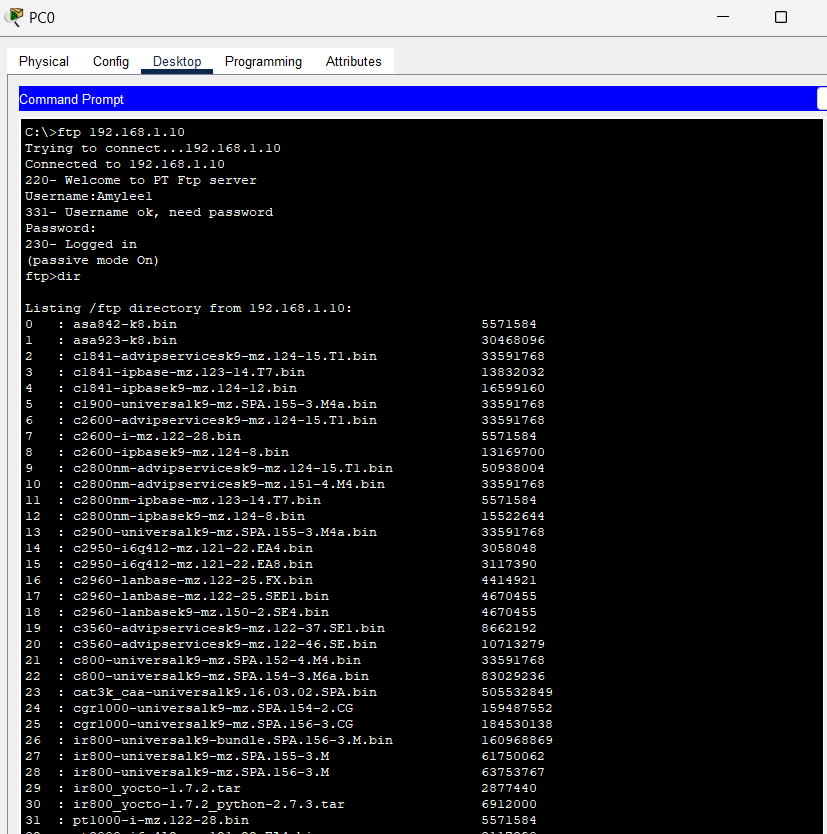


Figure 17: List of all the files

**CONCLUSION:**

The FTP server is successfully configured and ready to list, download or upload files.

**LAB 8**

**TITLE:** CONNECTION TWO PC’S USING RJ45 CABLE (ETHERNET CABLE)

**BACKGROUND THEORY:**

Connection two PC’s with an RJ45 cable create a small LAN without needing any switches or routers. By manually assigning IP addresses and configuring network settings, both computers can share and communicate directly. This setup is based on Ethernet standards, IP addressing and peer-to-peer networking principles.

**NETWORK DEVICES REQUIRED:**

* 2PCs or laptop with Ethernet port
* 1 Ethernet cable crossover cable
* Administrator access on both PCs

**PROCESS:**

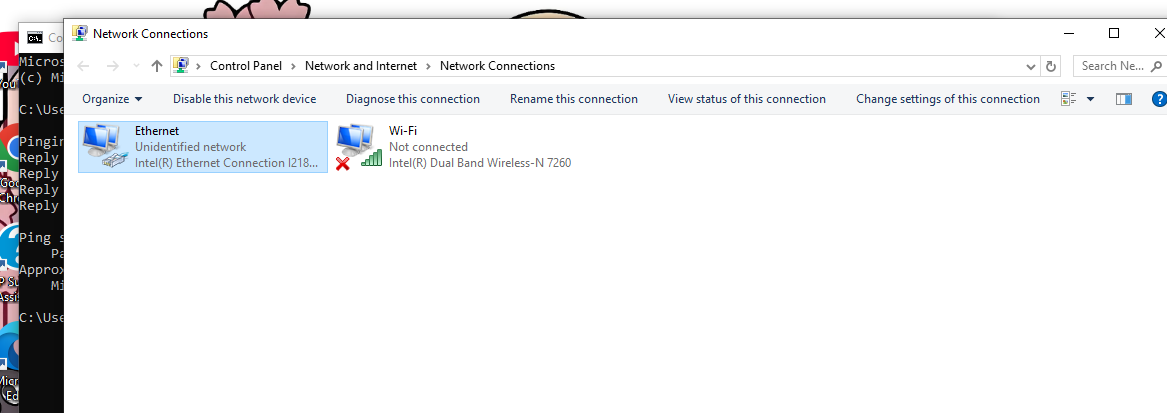
Step 1: Connect two laptops with RJ45 cable

* Ping one end of the RJ45 cable into the LAN port of laptop1.
* Ping the other end into the LAN port of laptop2.

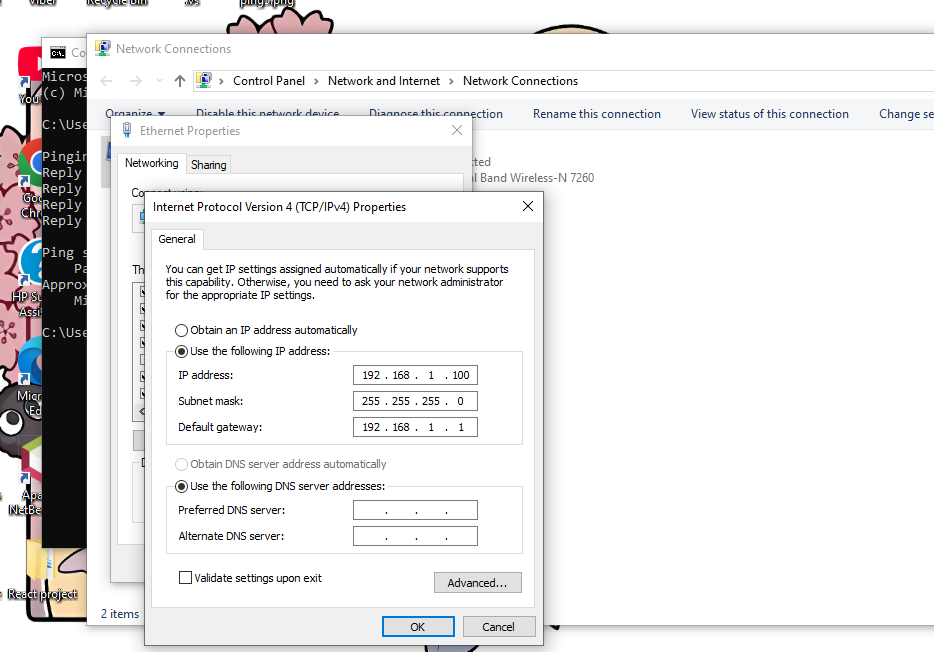
Step 2: Assign IP addresses manually.

On laptop1:

* Open control panel -> network and sharing center
* Click change adapter settings.
* Right click on Ethernet -> properties



* Click on internet protocol version 4 -> properties
* Assign IP addresses and subnet mask.
* Click to save

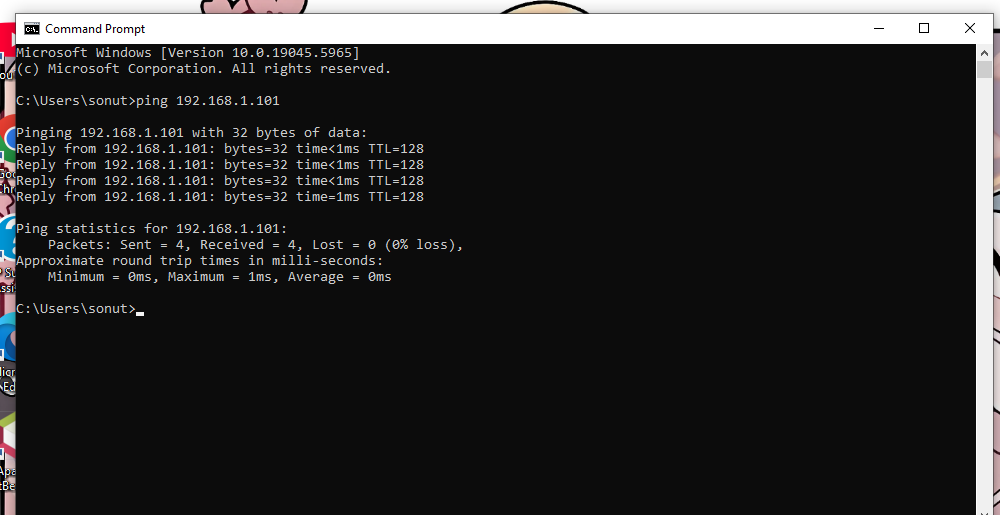


On laptop2:

* Repeat same steps.
* Set IP address(192.168.1.101)
* Click OK

Step 3: Test connection (ping)

* On laptop1, open command prompt
* Type ping and IP address of laptop2(192.168.1.101)

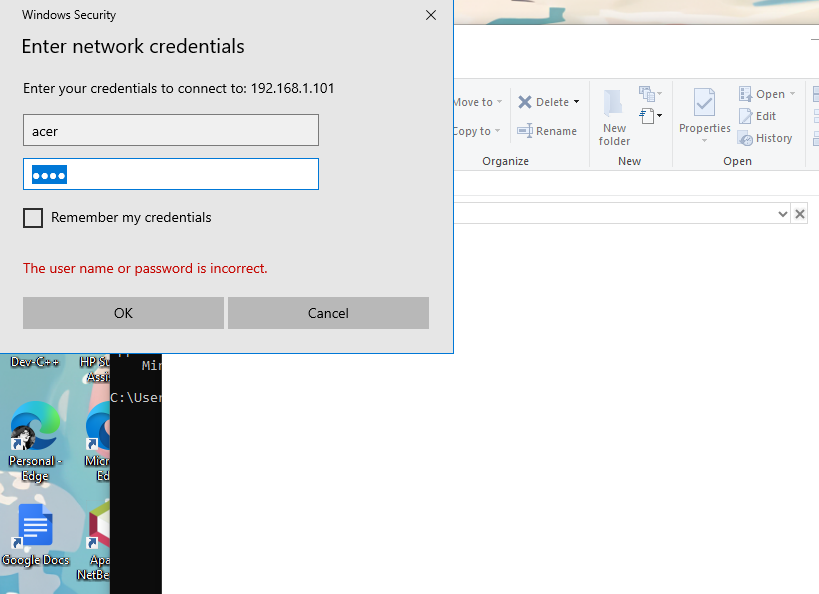


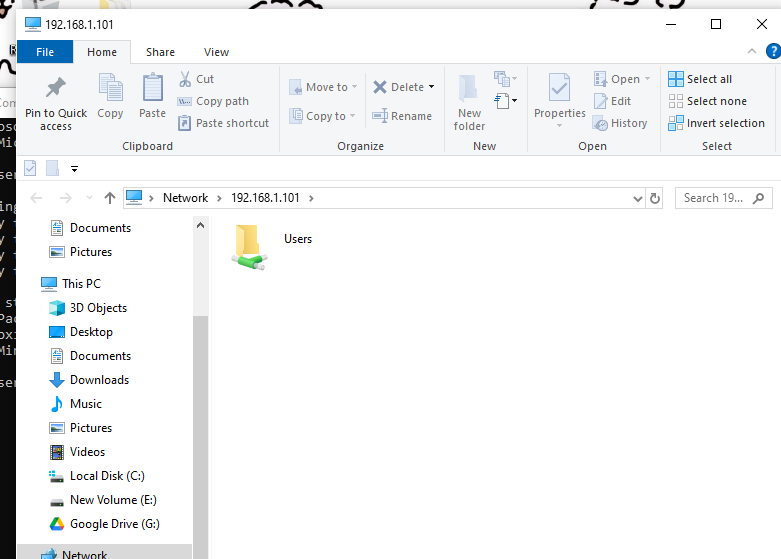
**OBSERVATION:**

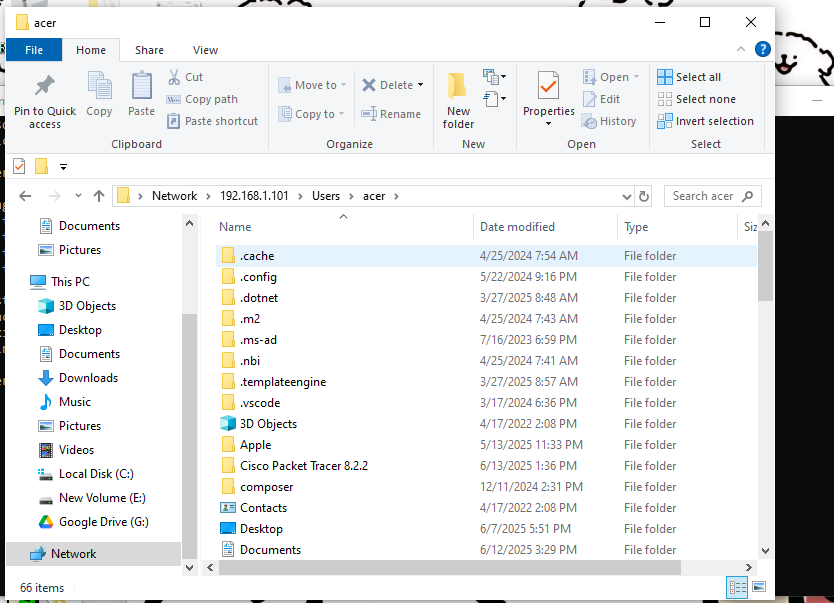
Reply from 192.168.1.101 , connection working.

Step 4: Share and access file between laptops

* Enable file sharing on both laptops.
* Open command prompt on laptop1 and type IP address of laptop2.
* Click ok.
* For connection u should enter laptop2 username and password
* Now we can access laptop2 and share files.







**CONCLUSION**

Connecting two laptops using a RJ45 Ethernet cable is a simple and effective method for creating a direct local network without needing a switch or router.

**LAB 10**

**TITLE:** INTRODUCTION TO WIRESHARK

**BACKGROUND THEORY:**

Wireshark is a free and open-source network protocol analyser. It is used to capture network packets and display the packet data in detail. This helps network administrators, security analysts, and students understand how data travels through networks.

Common protocols we can analyse are:

* Ethernet (Data Link Layer)
* IP, ICMP (Network Layer)
* TCP, UDP (Transport Layer)
* HTTP, DNS, FTP (Application Layer)

**OBJECTIVE:**

* To understand the basics of Wireshark.
* To learn how to capture and analyse network packets in real-time.
* To identity different types of protocols in network traffic (e.g. Ethernet, IP, TCP, HTTP).

**REQUIREMENTS:**

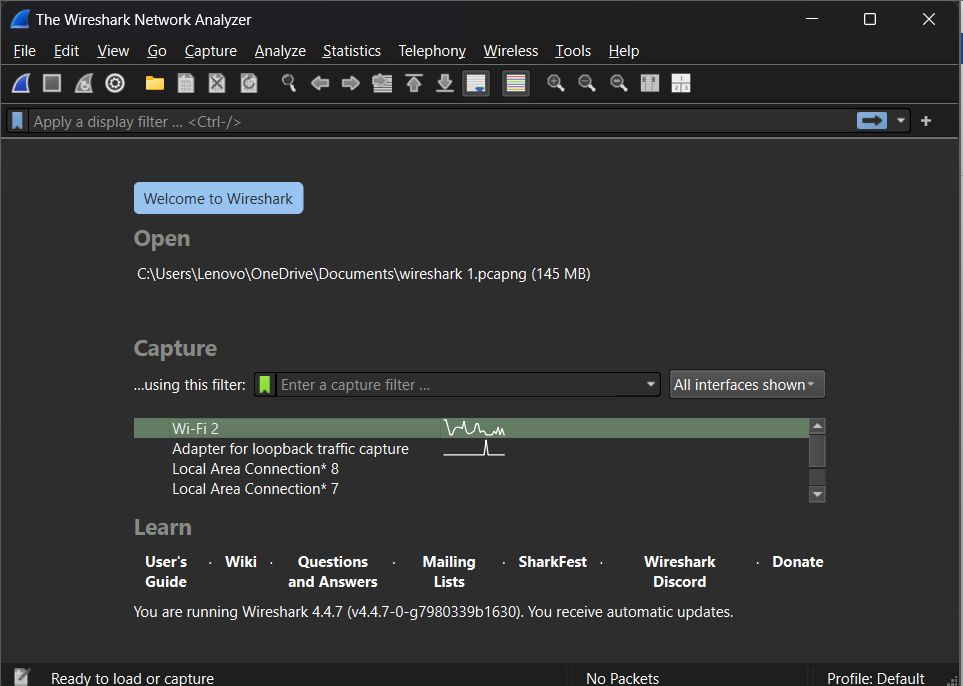
* Wireshark(latest version)
* A laptop with internet connection
* Any web browser (e.g. chrome)

**PROCEDURE:**

Step 1: Install Wireshark from <https://www.wireshark.org>.

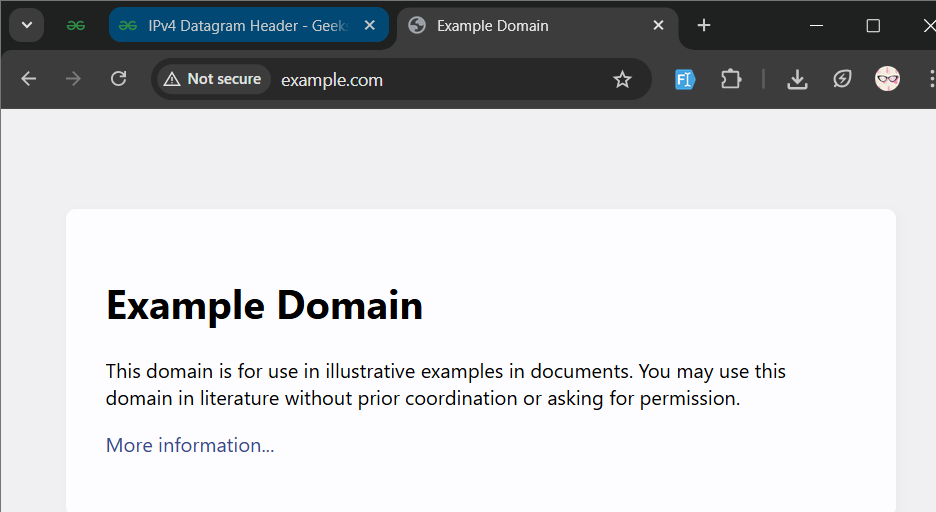
Step 2: Start capture:

* Launch Wireshark
* Select the active network interface(e.g. WI-FI)
* Click the start capture button.



Step 3: Generate Traffic

* Open a browser and visit a website (e.g. <http://example.com>).



Step 4: Apply filters

* http: to see HTTP traffic

Step 5: Stop capture (red square icon)

Step 6: Analyze packets:

* Click on any packet to see its detailed headers.

**RESULT:**

Successfully captured and filtered real-time packets using Wireshark.

**CONCLUSION**

Wireshark is a powerful tool for understanding network protocols and traffic. This lab helped gain hands-on experience in capturing and analyzing live packets and identifying how communication takes place at different layers of the OSI model.

**LAB 11**

**TITLE:** ANALYZING HTTP PROTOCOL USING WIRESHARK

**BACKGROUND THEORY:**

HTTP (Hypertext Transfer Protocol) is an application-layer protocol used for transmitting hypermedia documents, such as HTML. It follows a request-response model and is the foundation of data communication on the web.

Common HTTP Methods:

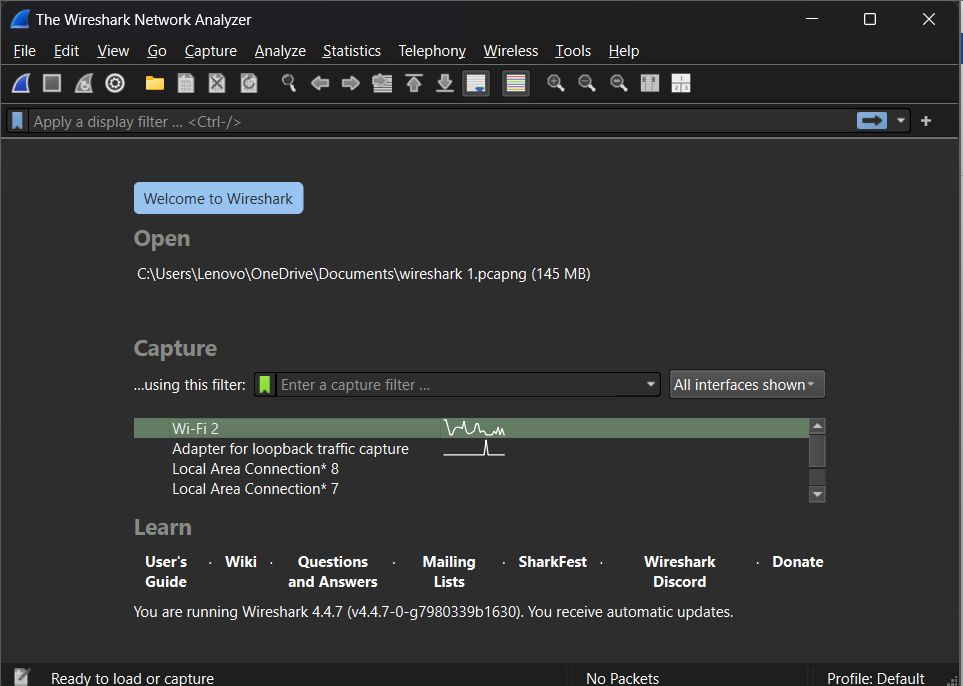
* GET – Request data from a server
* POST – Send data to a server
* Response Codes – 200 OK, 404 Not Found, 403 Forbidden, etc.

**TOOLS REQUIRED:**

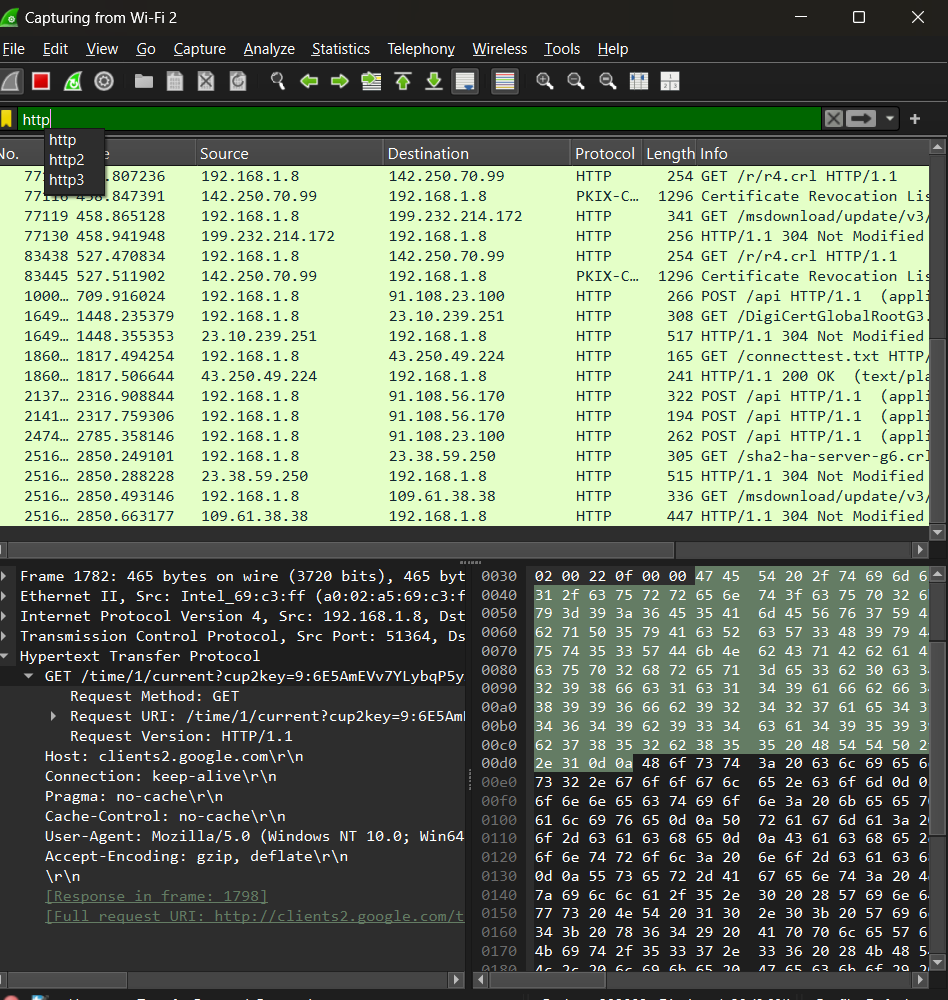
* Wireshark
* Web browser
* Internet connection

**PROCEDURE**

Step 1: Open Wireshark and select network interface i.e WIFI



Step 2: In the display filter bar, apply HTTP filter.

****

**RESULT:**

We have successfully captured HTTP request and response packets. The verified usage of GET method is observed.

**CONCLUSION:**

Wireshark is a powerful tool to monitor and analyze network traffic. This lab helped understand how HTTP operates at the application layer and how web communication takes place.

**LAB 12**

**TITLE:** USING ALL THE FILTERS IN WIRESHARK

**BACKGROUND THEORY:**

Wireshark is a free and open-source network protocol analyser. It is used to capture network packets and display the packet data in detail. This helps network administrators, security analysts, and students understand how data travels through networks.

Common protocols we can analyse are:

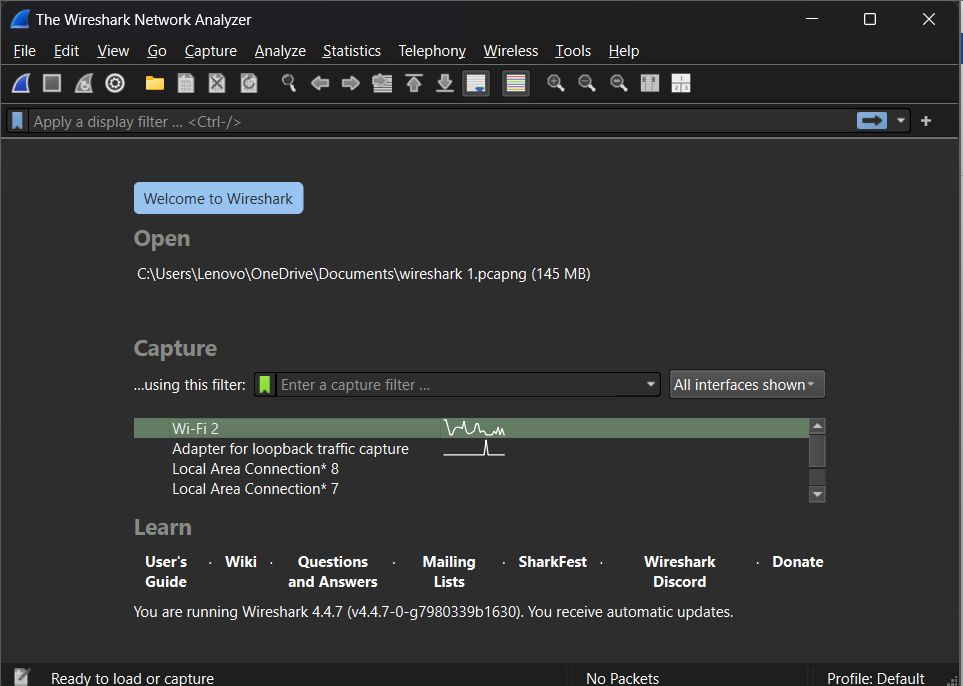
* Ethernet (Data Link Layer)
* IP, ICMP (Network Layer)
* TCP, UDP (Transport Layer)
* HTTP, DNS, FTP (Application Layer)

**TOOLS REQUIRED:**

* Wireshark
* Web browser
* Internet connection

**PROCEDURE**

Step 1: Open Wireshark and select network interface i.e WIFI

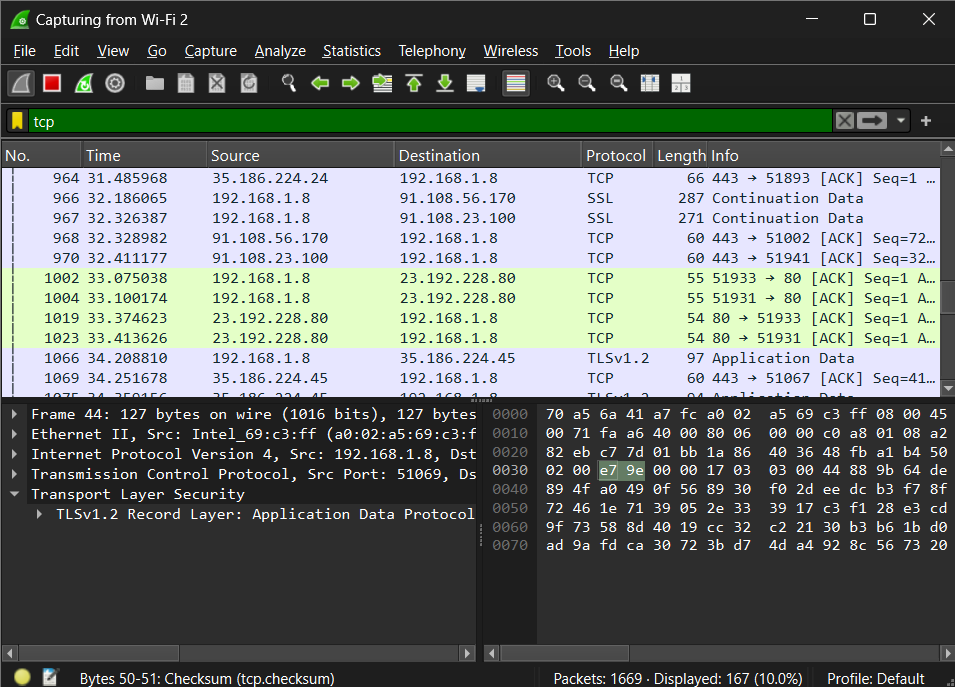


Step 2: In the display filter bar, apply filters.

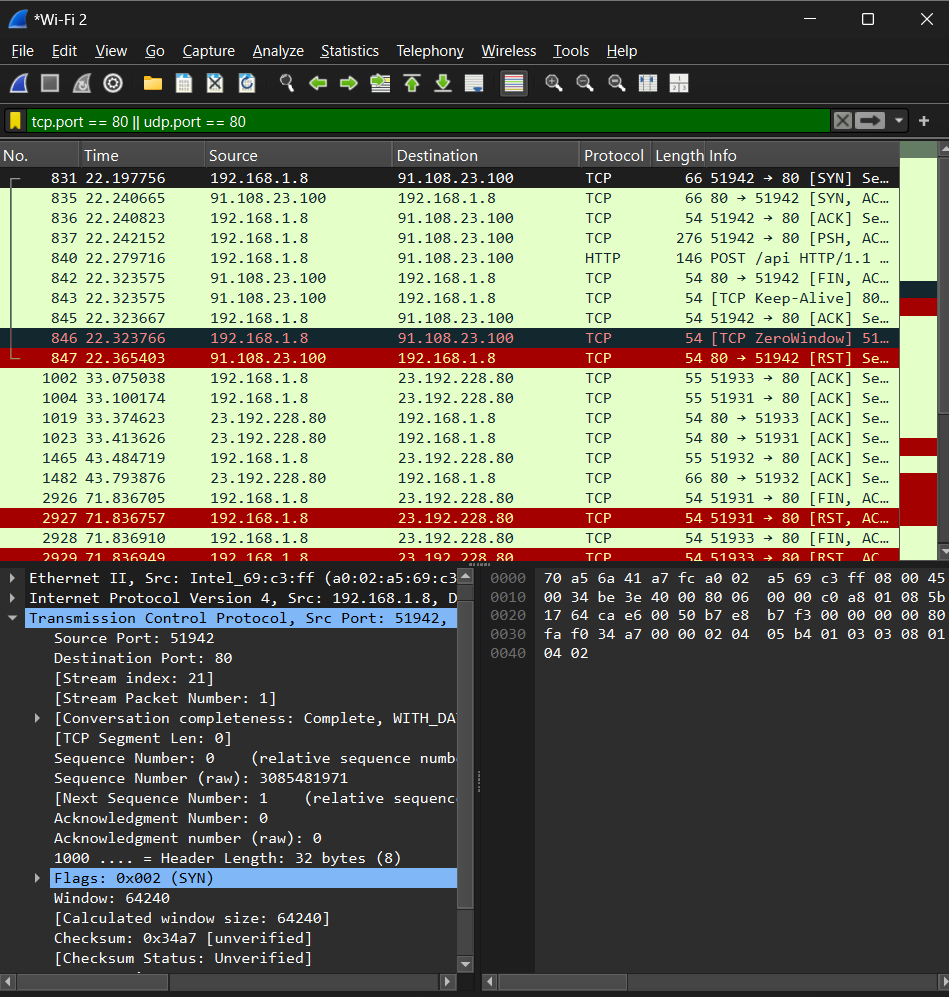
Filters commonly used are:



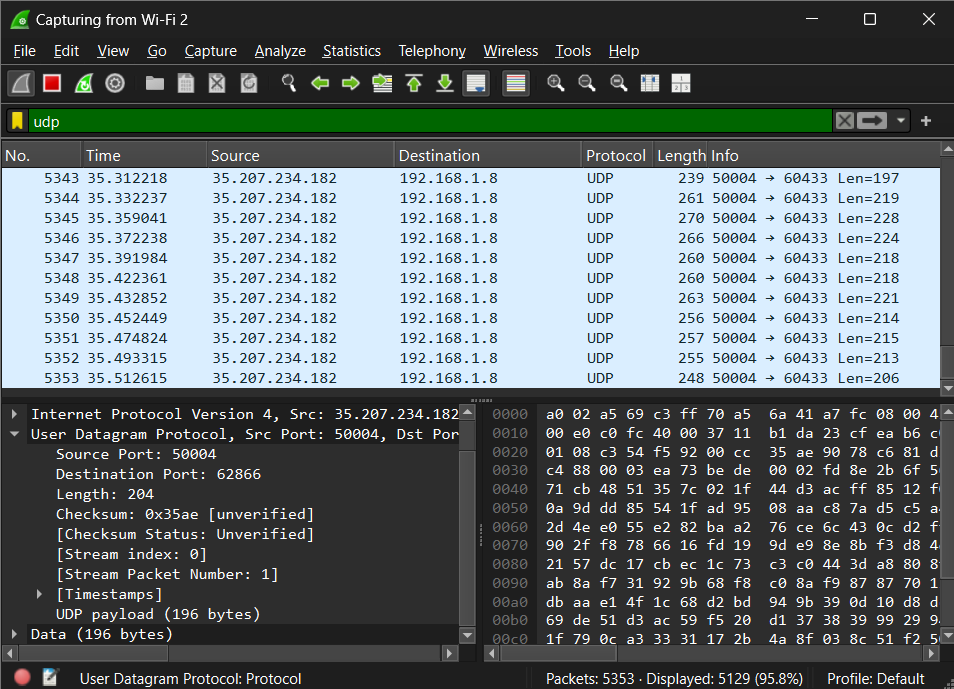
i. TCP (Shows all the TCP traffic)



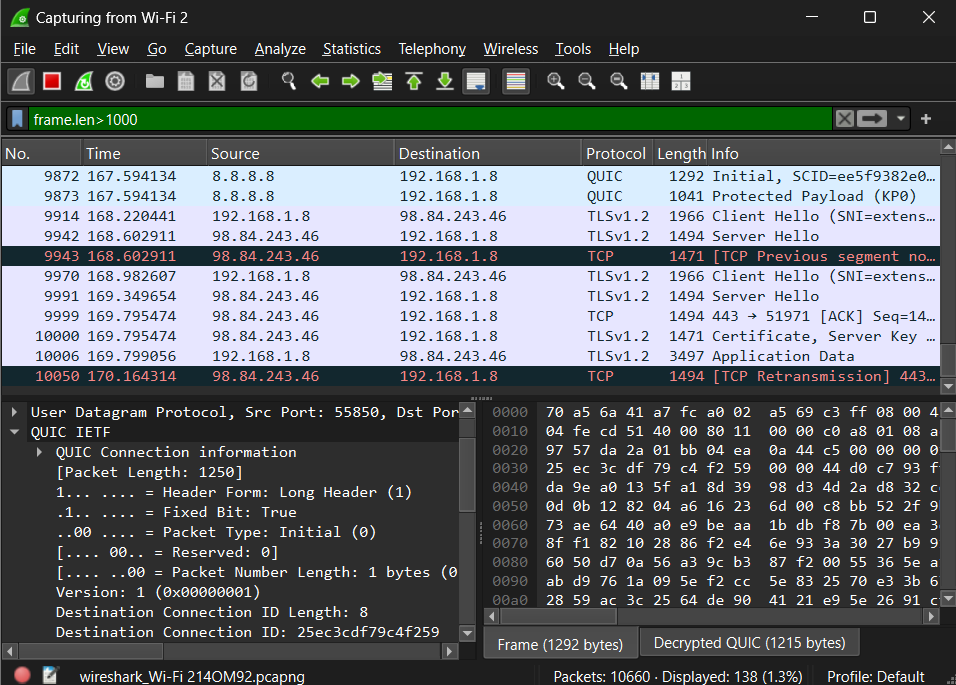
ii. tcp.port == 80 || udp.port == 80



iii. udp



iv. frame.len>1000



**CONCLUSION:**

Wireshark is a powerful tool to monitor and analyze network traffic.