

MIT	Academy of Engineering	INDEX & CERTIFICATE	
AN AUTONOMOUS INSTITUTE		ACADEMIC YEAR	2021-2022
Alandi (D), Pune – 412105		SEM/TRI	VI
DEPARTMENT OF E&TC ENGG.		CLASS & BLOCK	TY

Experiment no	Title	Mappe d CO	Page no	Assess ment points	Remark
01	Network commands & IP address configurations.	CO.1	3		
02	Fault detection of Cable tester for of UTP-CAT5 Cross / Straight LAN cable.	CO.1	6		
03	Implementation of LAN using star topology and connectivity between two computers using cross over UTP CAT5 cable.	CO.1	9		
04	Installation and configuration of Web Server and hosting web page using HTML programming	CO.3	12		
05	Configure network topology using packet tracer.	CO.2	17		
06	Configure network using Application layer protocols (DNS, HTTP, DHCP)	CO.3	20		
07	Configuration of TELNET using packet tracer.	CO.2	30		
08	Configure network using Distance Vector Routing Protocol.	CO.3	37		
09	Configure network using Link State vector routing protocol.	CO.3	41		
10	Mini Project 1. Connection and configuration of a basic switch. 2. Configuration of basic router. 3. Setup an email server.	CO.1 CO.2 CO.3			

CERTIFICATE

This is to certify that Master Anirudh Khabya Roll No TEE16 has successfully completed the experiments for the course Digital Systems and Applications for academic year 2021-22.

Sign AKi

Student Anirudh Khabya

Sign

Course instructor

Expt.No.1**Date: 15/04/2022****Network commands & IP address configurations**

Objective:

- Study of basic network command and Network configuration commands

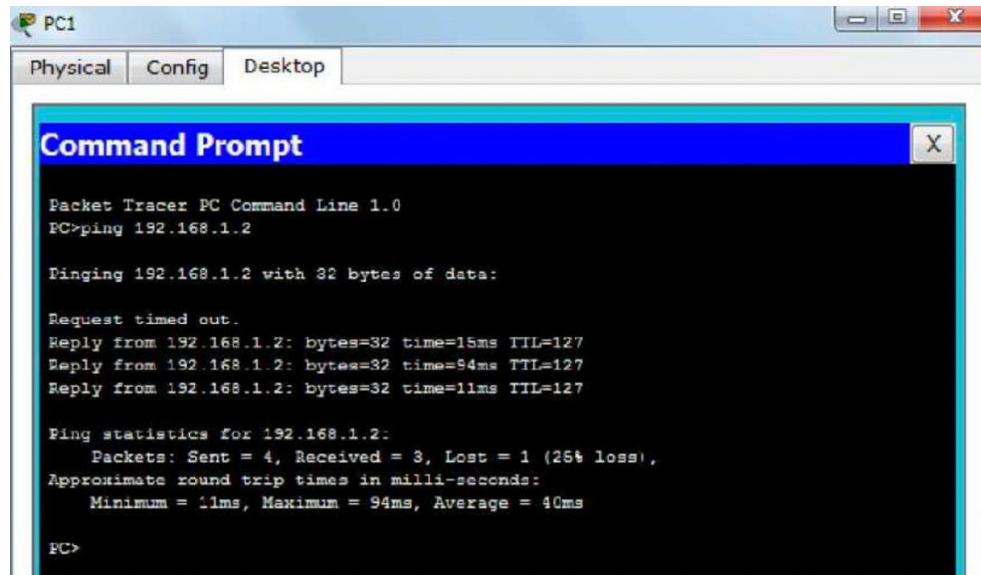
Requirements

- Command Prompt and Packet Tracer

Procedure:

To do this EXPERIMENT- follows these steps:

- In this EXPERIMENT- students have to understand basic networking commands e.g ping, tracert etc.
- All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.
- These commands includes:
- Configuring the Router commands
- General Commands to configure network
- Privileged Mode commands of a router
- Router Processes & Statistics
- IP Commands
- Other IP Commands e.g. show ip route etc.
- **Ping:**
- ping(8) sends an ICMP ECHO_REQUEST packet to the specified host. If the host responds, you get an ICMP packet back. Sound strange? Well, you can "ping" an IP address to see if a machine is alive. If there is no response, you know something is wrong.



```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=15ms TTL=127
Reply from 192.168.1.2: bytes=32 time=94ms TTL=127
Reply from 192.168.1.2: bytes=32 time=11ms TTL=127

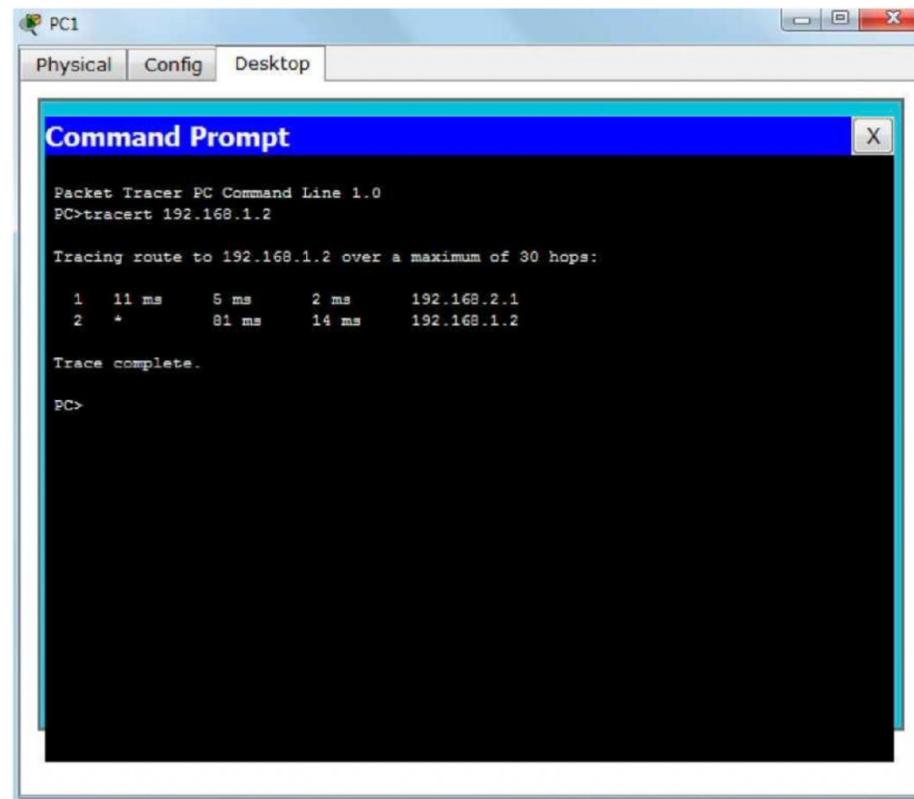
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 94ms, Average = 40ms

PC>

```

- **Trace route:**

- Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.



```

Packet Tracer PC Command Line 1.0
PC>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:
  1  11 ms      5 ms      2 ms      192.168.2.1
  2  *          81 ms     14 ms      192.168.1.2

Trace complete.

PC>

```

- **nslookup:**

- Displays information from Domain Name System (DNS) name servers.

- NOTE: If you write the command as above it shows as default your pc's server name firstly.

- **pathping:**

- A better version of tracert that gives you statics about packet lost and latency.

```
C:\Users\lenovo>pathping 192.168.1.12
Tracing route to 192.168.1.12 over a maximum of 30 hops
  0  lenovo-PC.dronacharya [192.168.1.9?]
  1  lenovo-PC.dronacharya [192.168.1.9?]  reports: Destination host unreachable.

Computing statistics for 25 seconds...
          Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0          lenovo-PC.dronacharya [192.168.1.9?]
  1  ---      100/ 100 =100%    0/ 100 = 0%  lenovo-PC [192.168.1.9]

Trace complete.
C:\Users\lenovo>
```

- **Getting Help**

- In any command mode, you can get a list of available commands by entering a question mark (?).

- **Router>?**

- To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?).

- **Router#co?**

- configure connect copy

- To list keywords or arguments, enter a question mark in place of a keyword or argument.

- Include a space before the question mark.

- **Router#configure ?**

- memory Configure from NV memory network Configure from a TFTP network host terminal

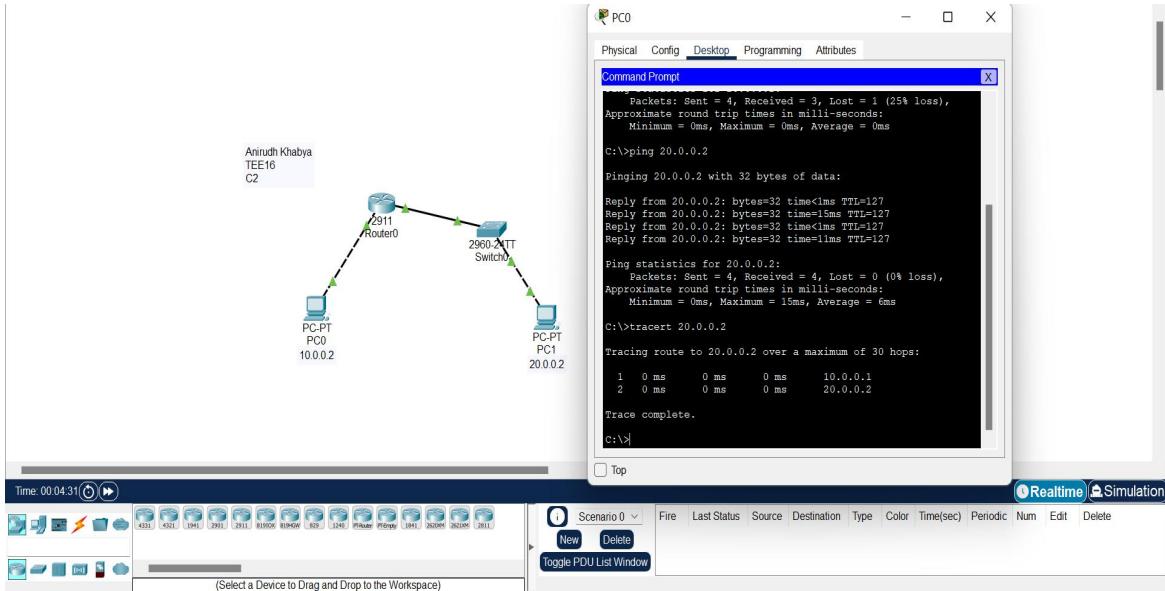
- Configure from the terminal

- You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the show command to sh.

- **Configuration Files**

- Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the start-up configuration. Use the following privileged mode commands to work with configuration files.

Output of ping and tracert



Conclusion:

In this experiment, we have seen various network administration command-line utilities like ping, tracert along with their syntax and examples. We have also gone through IP address and learned how to configure it. We have downloaded and installed cisco packet tracer and made basic circuit on it. We have performed above mentioned practically and successfully.

Expt.No.2**Date: 15/04/2022**

Fault detection of Cable tester for of UTP-CAT5 Cross / Straight LAN cable.

Objective:

- Study of different types of Network cables and practically implement the cross-wire cable and straight through cable using clamping tool.
- Fault detection of Cable tester for of UTP-CAT5 Cross / Straight LAN cable.
-

Requirements:

- RJ-45 connector, Clamping Tool, Twisted pair Cable, cable tester

Procedure:

To do these practical following steps should be done:

- Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render it useless.
- Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.
- Spread the wires apart but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket.
- Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.
- You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end.
- Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

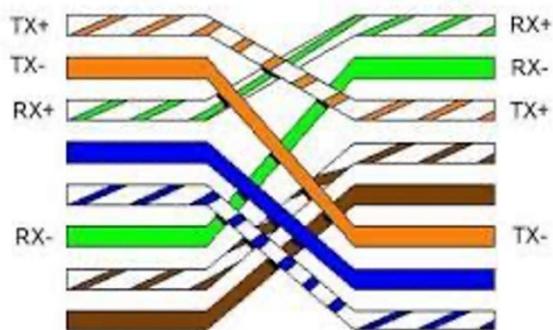
Diagram shows you how to prepare straight through wired connection:

Defining Ethernet LANs: Standard Names				
Original IEEE	IEEE Shorthand Name	Informal Name(s)	Speed	Typical Cabling
802.3i	10BASE-T	Ethernet	10 Mbps	UTP
802.3u	100BASE-T	Fast Ethernet (Fast E)	100 Mbps	UTP
802.3z	1000BASE-X	Gigabit Ethernet (Gig E, GbE)	1000 Mbps	Fiber
802.3ab	1000BASE-T	Gigabit Ethernet (Gig E, GbE)	1000 Mbps	UTP
802.3ae	10GBASE-X	10 GbE	10 Gbps	Fiber
802.3an	10GBASE-T	10 GbE	10 Gbps	UTP
802.3ba	40GBASE-X	40GbE (40 GigE)	40 Gbps	Fiber
802.3ba	100GBASE-X	100GbE (100 GigE)	100 Gbps	Fiber

TIA/EIA 568B Wiring

1		White and Orange
2		Orange
3		White and Green
4		Blue
5		White and Blue
6		Green
7		White and Brown
8		Brown

TIA/EIA 568B Ethernet Crossover Cable Wiring



Conclusion:

In this experiment, we have seen various types of cables such as UTP and Straight and differentiated them. We get to know many related terms such as Clamping Tool, Twisted pair Cable, Cable tester. The video shown was self explainable which include how to configure above mentioned cables. We also gone in details about switches and Router.

Expt.No.3**Date: 15/04/2022**

Implementation of LAN using star topology and connectivity between two computers using cross over UTP CAT5 cable.

Objective

- Build a small network using Windows 2003 Operating System.
- Install TCP/IP.
- Manually configure TCP/IP parameters.
- Use the IPCONFIG utility to view configured IP parameters.
- Use the PING utility to test TCP/IP communications and its different options.
- Share a folder.
- Connect to a shared folder.

Requirements

- Personal computers with Network Interface Cards connected through category 5 UTP cables.
- Windows 2003 lab server 196.15.60.220.
- Windows 2003 advanced server Operating Systems installed on each computer.
- A shared folder named Samples should be created on the LAB SERVER computer.
- Students are provided with local administrator account.

Theory

Operating System:

An operating system (OS) is software, consisting of programs and data, that runs on computers, manages computer hardware resources, and provides common services for execution of various application software. The operating system is the most important type of system software in a computer system. Without an operating system, a user cannot run an application program on their computer, unless the application program is self booting.

For hardware functions such as input and output and memory allocation, the operating system acts as an intermediary between application programs and the computer hardware, although the application code is usually executed directly by the hardware and will frequently call the OS or be interrupted by it. Operating systems are found on almost any device that contains a computer from cellular phones and video game consoles to supercomputers and web servers. Examples of popular modern operating systems are: BSD, Linux, MacOS, Microsoft Windows and UNIX.

A local area network(LAN):

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-TG. and also provide a way to create a wired LAN using existing home-wires (coaxial cables, phone lines and power lines).

All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called "layer 3 switches" because they only have Ethernet interfaces and must understand IP. It would be more correct to call the access routers, where the router at the top is a distribution router that connects to the Internet and academic networks' customer access routers.

Internet Protocol Suite:

The Internet Protocol Suite is the set of communications protocols used for the Internet and other similar networks. It is commonly also known as TCP/IP named from two of the most important protocols in it: the Transmission Control Protocol

(TCP) and the Internet Protocol (IP), which was the first two networking protocols defined in this standard.

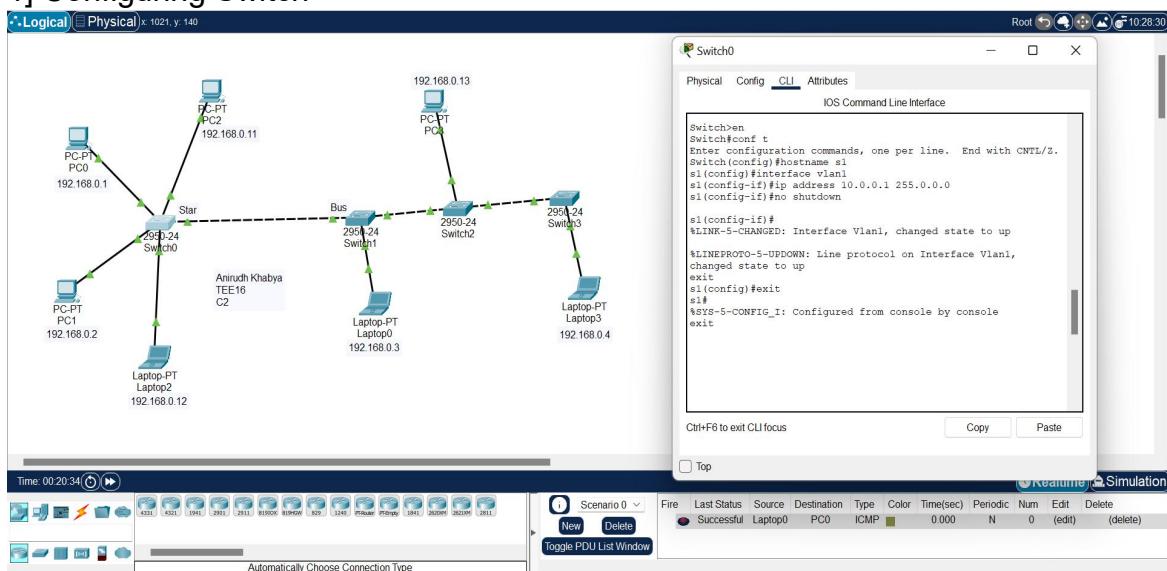
The Internet Protocol Suite consists of four abstraction layers. From the lowest to the highest layer, these are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer. The layers define the operational scope or reach of the protocols in each layer, reflected loosely in the layer names. Each layer has functionality that solves asset of problems relevant in its scope.

Procedure

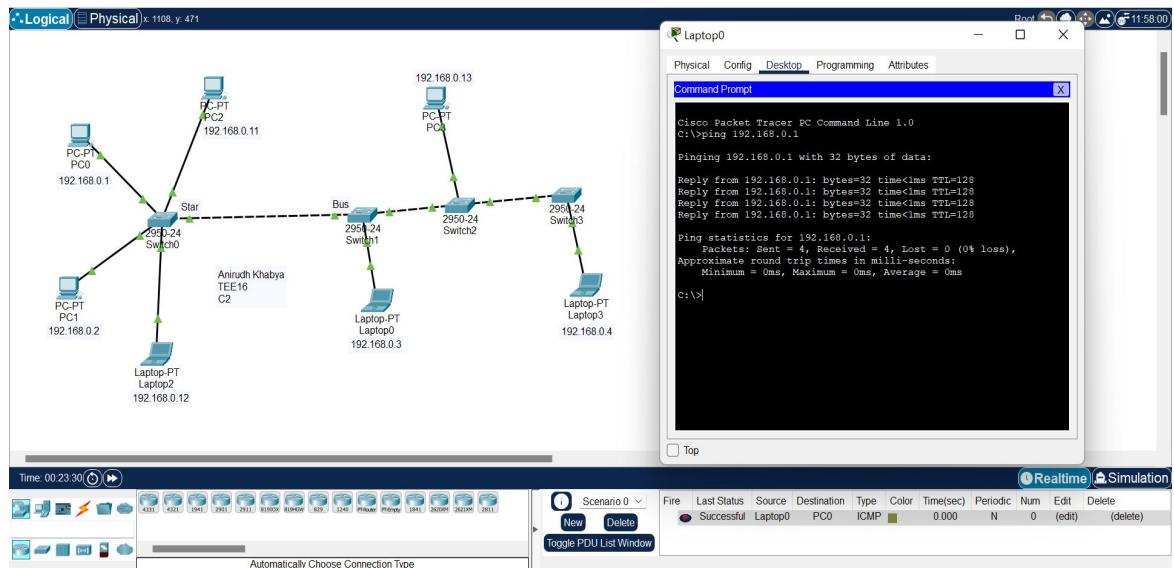
1. Install operating system on the PC
2. Insert/Plugged a one side of cat-5 Straight-cable at the NIC port/interface to the computer and other side to the HUB port
3. Select network neighborhood properties
4. Select local area connection properties
5. Select Internet protocol TCP/IP properties
6. Select Static IP address
7. Configure the IP address and the Subnet mask
8. Repeat the above 5-step for others computers
9. Ping the other computer by entering the hostname or IPaddress of other computer; from one computer to other computer to confirm the connectivity.

Output

1] Configuring Switch



2] Pinging



Conclusions:

In this experiment, using cisco packet tracer, we have implemented LAN using Star topology and connectivity between two computers using cross over UTP CAT5 cable. The result of the experiment has successfully come.

Expt.No.4

Date: 15/04/2022

Installation and Configuration of Web Server

Objective

- Install Microsoft Internet Information Server (IIS5)services
- Connect to a Web-server
- Verifying the installed IIS5 services
- Assign multiple IP addresses to the web-server

Requirements

- Computers in LAN
- Windows OS CD for IIS Installation
- Web Site Design tool (HTML, XML or Microsoft Front page,etc)

Theory

Internet Information Services (IIS):

It is a software services that support Web site creation, configuration, and management, along with other Internet functions. Internet Information Services include Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

Simple Mail Transfer Protocol (SMTP):

IT is a member of the TCP/IP suite of protocols that governs the exchange of electronic mail between message transfer agents.

File Transfer Protocol (FTP):

A member of the TCP/IP suite of protocols, used to copy files between two computers on the Internet. Both computers must support their respective FTP roles: one must be an FTP client and the other an FTP server.

Network News Transfer Protocol (NNTP):

A member of the TCP/IP suite of protocols used to distribute network news message to NNTP servers and clients (newsreaders) on the Internet. NNTP is designed so that news articles are stored on a server in a central database, thus enabling a user to select specific items to read.

Procedure

1. Install Windows-OS
2. Install graphics driver file after installation of Win-OS to improve resolution
3. Install Internet Information Service(IIS)
4. Install Microsoft office, Microsoft Front page
5. Design Web site or Web page in Microsoft Front page or HTML
6. Save the Site on the location (Like C: drive or E: drive,etc)
7. Open Internet Information Service and create virtual directory and load the web page or web site on the document option and go with the further setting
8. Access the site through another PC by typing "http://IP Address File name or site name"

Installing IIS

1. To install IIS, add optional windows components, or remove optional components
2. Click Start, click Control Panel, and click Add or Remove Program
3. Click Add, Remove Windows Components. The Windows Components Wizard appears
4. IIS requires that you install certain software on the computer prior to installation. Review the IIS Software Checklist below before installing IIS.

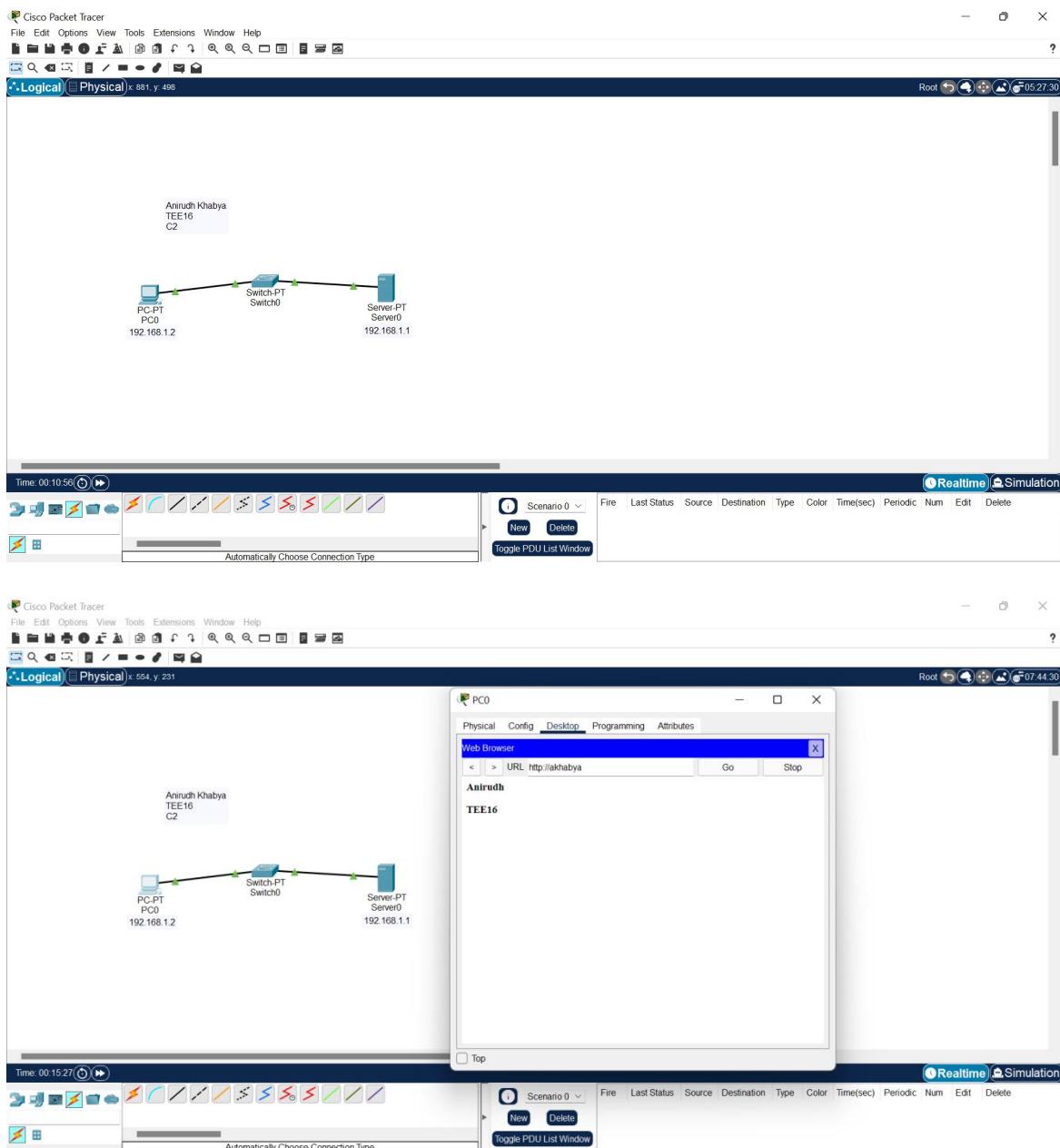
5. IIS Software Check list

6. Before you install IIS, you need to install the Windows TCPIP Protocol

The following optional components are recommended:

During installation, IIS installs optional components like Common Files, Documentation, and the Internet Information Services snap in. You can choose not to install the optional components; however, deselecting specific components can decrease IIS functionality or disable Services. If you are unfamiliar with the optional components and how they affect IIS, installed with heed fault settings. After you install IIS, you can view Installing IIS Optional Components in the IIS online documentation for more information.

Output:



Conclusions:

In this experiment, we have learned to install and configure a web server. Also hosted web page using html programming. Web server is basically a computer that usually runs websites. Web hosting is basically a process of using a server to host website. It enables website to be accessible to users via internet. It provides services to other devices or programs in network. We successfully get the result.

Expt.No.5**Date: 15/04/2022**

Configure network topology using packet tracer

Objective

- Configure network topology using packet tracer

Requirements

Command Prompt and Packet Tracer.

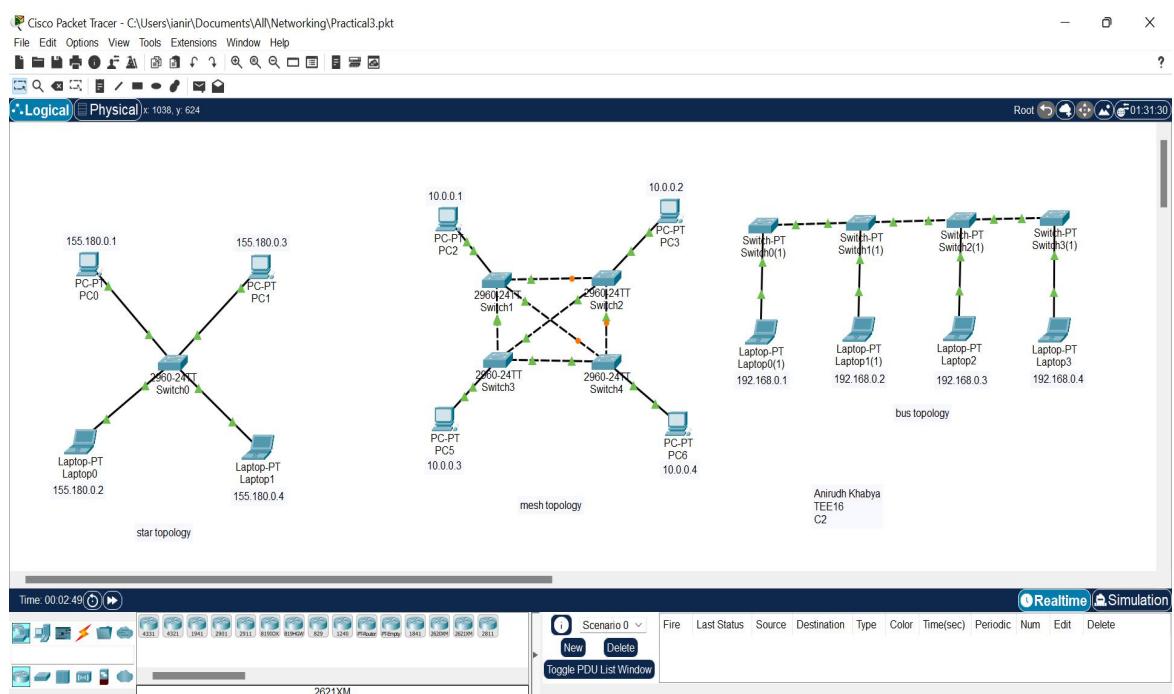
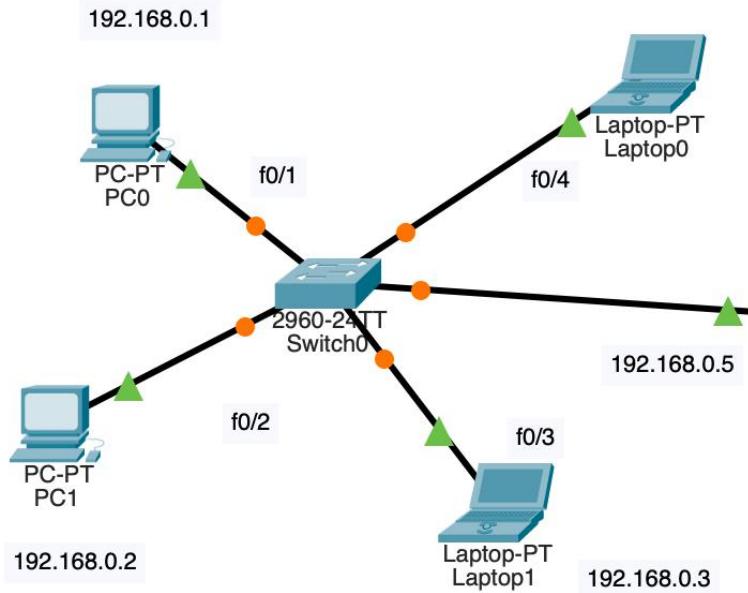
Theory:

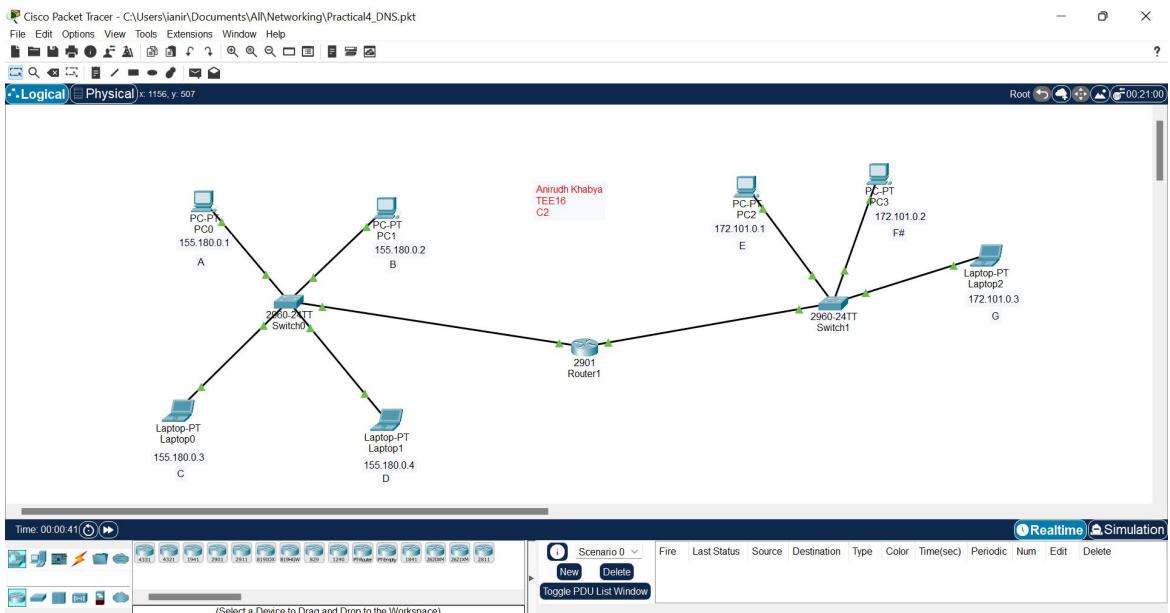
Layers associated while configuring LAN

- **Physical Layer:**
 - Defines physical characteristics of medium used to transfer data between devices E.g voltage levels, maximum transmission distance, physical connectors, cable specifications
 - Bits converted into electrical or radio signals
- **Data Link Layer:**
 - Provides node- node connectivity and data transfer (PC-sw;sw-sw; sw-router; router-router)
 - Defines how data is formatted for transmission over a physical medium
 - Detects and corrects physical layer errors
 - Layer 2 address- MAC address is involved

Ethernet Frame Format:

7 byte	1 byte	6 byte	6 byte	2 byte	46 to 1500 byte	4 byte
Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	Data	Frame Check Sequence (CRC)





Conclusion

In this experiment, we have made different types of network topologies. By choosing the topology best suited for your organization, its resources, and its needs, you can reduce operational costs, improve performance, and optimize resource allocation.

Expt.No.6**Date: 15/04/2022**

Configure network using Application layer protocols (DNS, HTTP, DHCP)

Objective

- Determine the local host address.
- Ping to a host using his Net BIOS name.
- Configure IP address using DHCP server.
- Configure DNS service on CCNA Packet Tracer server.
- Use Domain Name Service to resolve host names into IP addresses.
- Interact with a server using HTTP protocol .

Requirements

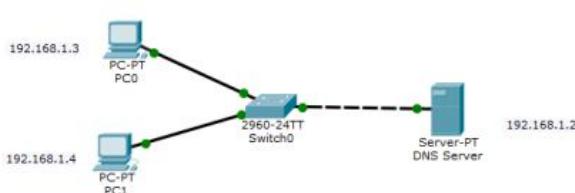
- Personal computers with Network Interface Cards connected through category 5 UTP cables.
- CCNA Packet Tracer
- Windows 2000 Network Operating System installed in each computer.
- TCP/IP protocol installed in each computer.
- Each computer should have an IP address 196.15.60.x where x is the computer's number.
- Students are provided with local administrator account.
-
- The lab server server2000 (196.15.60.220) is configured as DNS server for the domain name nwlab.edu with plenty of records.
- Email server installed on Server2000 (196.1560.220).

Part A: Configure the DHCP service.

- From the customer workstation, use a console cable and terminal emulation software to connect to the console of the customer Cisco1841 ISR.
- Log in to the console of the Cisco 1841 ISR and enter global configuration mode.
- Before creating a DHCP pool, configure the addresses that are excluded. The range is from 192.168.1.1 to 192.168.1.49.
- Customer Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.
- Create a DHCP pool called pool1.
- Customer Router(config)#ip dhcp pool pool1
- Define the network address range for the DHCP pool.
- CustomerRouter(dhcp-config)#network 192.168.1.0 255.255.255.0
- Define the DNS server as 192.168.1.10.
- CustomerRouter(dhcp-config)#dns-server 192.168.1.10
- Define the default gateway as 192.168.1.1.
- CustomerRouter(dhcp-config)#default-router 192.168.1.1
- Add an exclusion range of 192.168.1.1 to 192.168.1.49 to the DHCP pool.
- CustomerRouter(dhcp-config)#exit
- Customer Router(config) #ip dhcp excluded-address 192.168.1.1 192.168.1.49
- Exit the terminal.

Configure a DNS server in Packet Tracer.

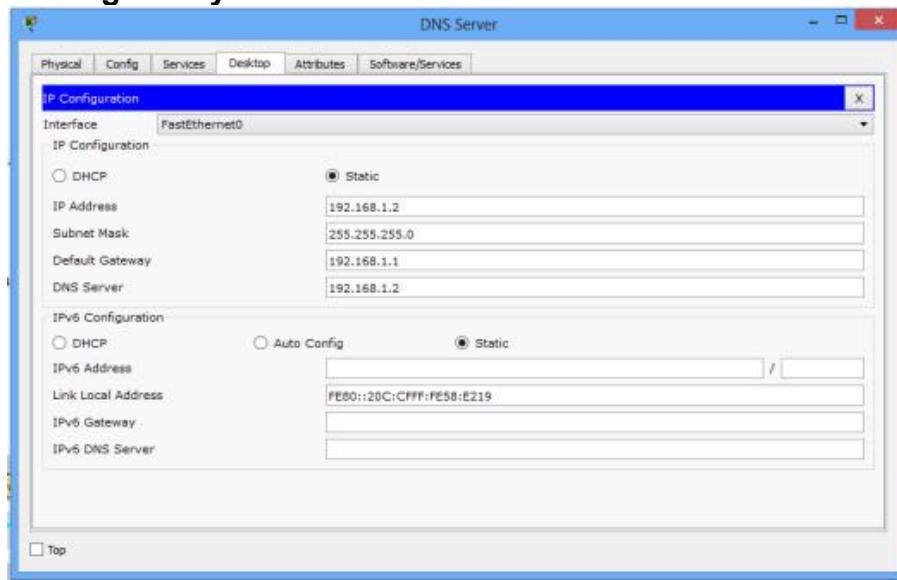
1. Build the network topology.



- 2. Configure static IP addresses on the PCs and the server.

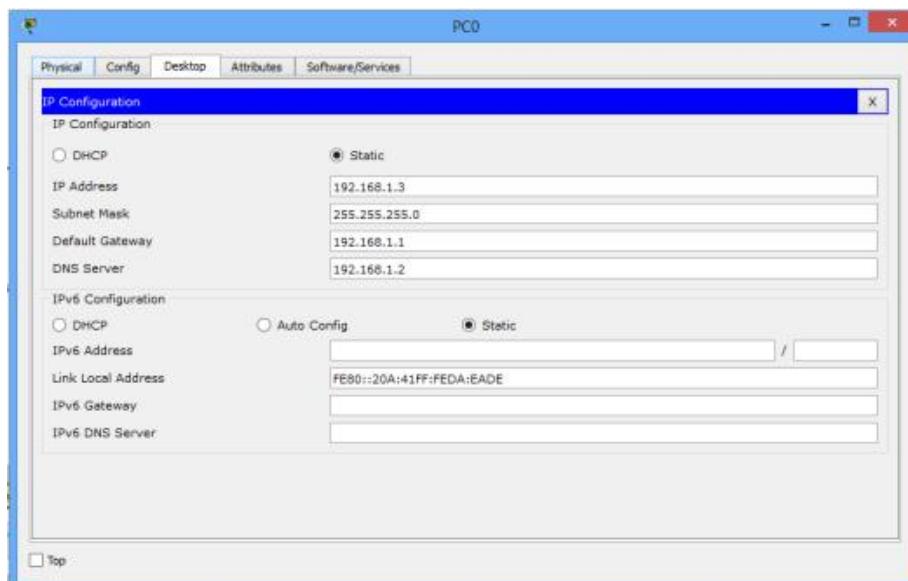
- **Server**

- **IP address:** 192.168.1.2 **Subnet mask:** 255.255.255.0 **Default gateway:** 192.168.1.1 **DNS Server:** 192.168.1.2



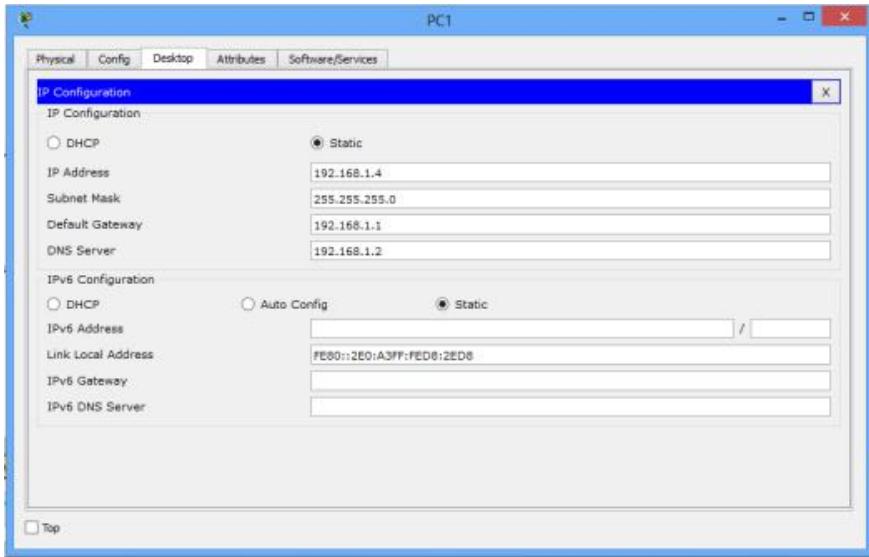
PC0

IP add: 192.168.1.3 **Subnet mask:** 255.255.255.0 **Default gateway:** 192.168.1.1 **DNS server:** 192.168.1.2



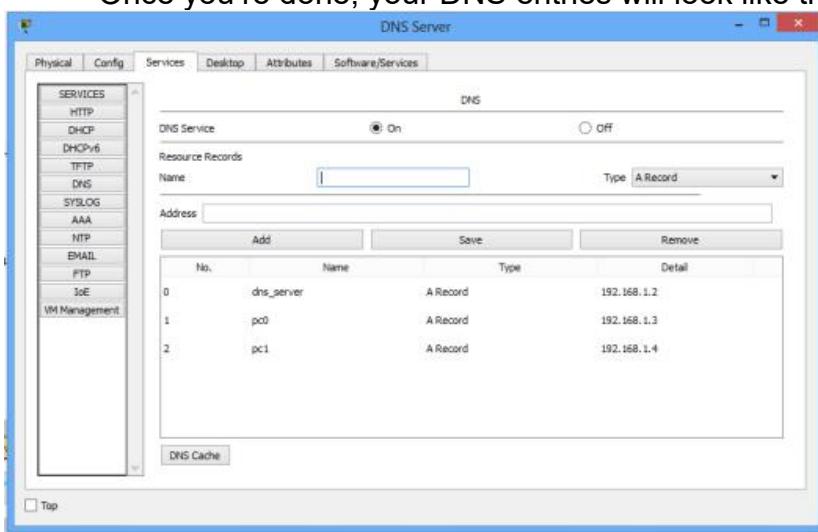
PC1

IP address: 192.168.1.4 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 DNS Server: 192.168.1.2



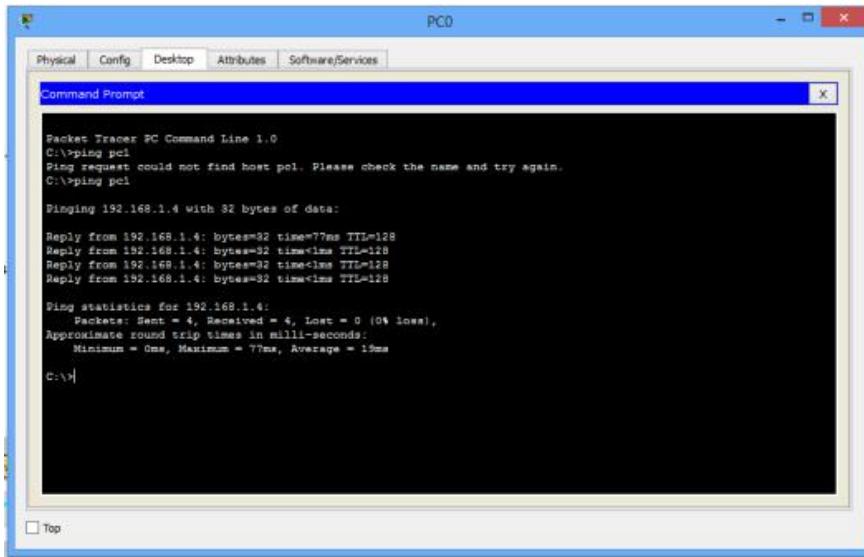
3. Configure DNS service on the generic server.

- To do this, click on the server, then Click on Services tab.
- Click on DNS server from the menu.
- First turn ON the DNS service, then define names of the hosts and their corresponding IP addresses.
- For example, to specify the DNS entry for PC0: In the name and address fields, type:
- Name: PC0 Address: 192.168.1.3
- Click on add then save. Repeat this for the PC1 and the server.
- Once you're done, your DNS entries will look like this:



Finally,

4. Test domain name – IP resolution. Ping the hosts from one another using their names instead of their IP addresses. If the DNS service is turned on and all IP configurations are okay, then ping should work.
- For example, ping PC1 from PC0. Ping should be successful.



Configure a HTTP server in Packet Tracer

For this go to :

- server >services>Http>select both services as on mode.
- Now we can search webpage from any connected PC. This will so you only existing HTTP file when you put Server IP.
- Go to any PC>Desktop>Web Browser>put server IP(192.168.1.1)> click Enter.
- It will so you below result.

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://192.168.1.1

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:

[A small page](#)

[Copyrights](#)

[Image page](#)

[Image](#)

- If you want to create your own webpage then it is very simple. Just follow path

- Go to on server>services>HTTP>new file>just write you html code whatsoever you want as I coded here.

The screenshot shows the 'Services' tab selected in the top navigation bar. On the left, a sidebar lists various services: Physical, Config, Services (selected), Desktop, Programming, Attributes. The main area displays a file editor with the following details:

- File Name:** myfirstwebpage.html
- Content:**

```
<h1>My First Web Page</h1>
<table border =10>
<tr><th>Student Name:</th><th>Andre</th></tr>
<tr><th>Contact:</th><th>451254812</th></tr>
</table>
```

- Then click on save button.
- You may not find your file when search from PC. For it select path Go to server>Services>HTTP>index.html>edit>write it as below.

The screenshot shows the 'Services' tab selected in the top navigation bar. On the left, a sidebar lists various services: Physical, Config, Services (selected), Desktop, Programming, Attributes. The main area displays a file editor with the following details:

- File Name:** index.html
- Content:**

```
<html>
<center><font size='2' color ='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscptologo177x111.jpg'>Image </a>
<br><a href='myfirstwebpage.html'>My First Web Page</a>
</html>
```

We can find now our created web page.

The screenshot shows a web browser window with the title "Cisco Packet Tracer". The URL bar contains "http://192.168.1.1". The page content is:

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

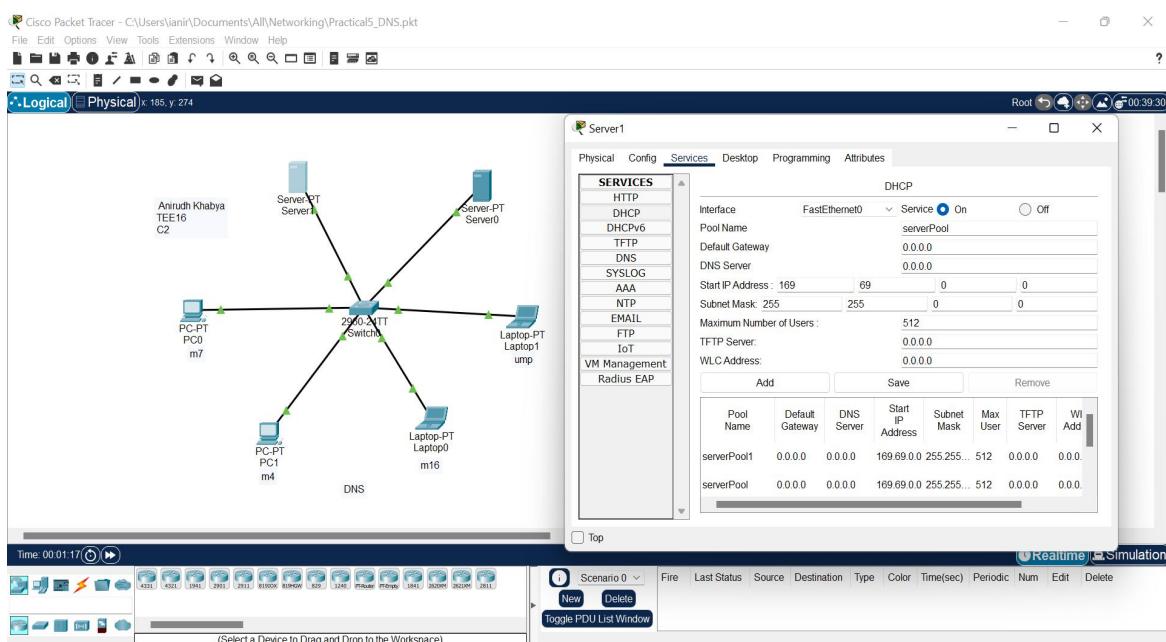
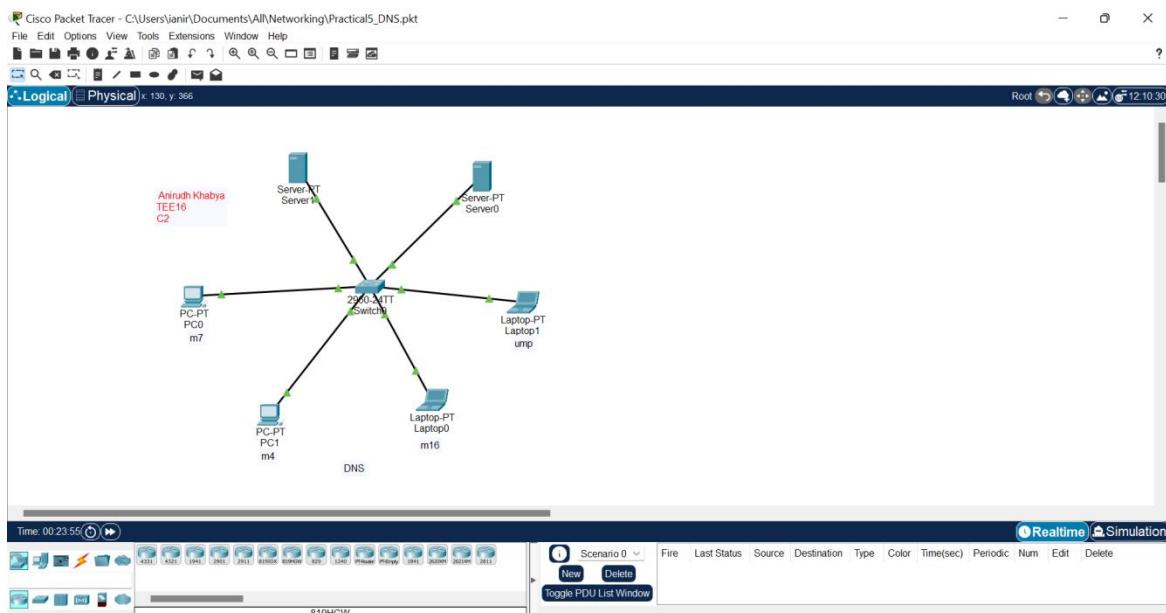
Quick Links:

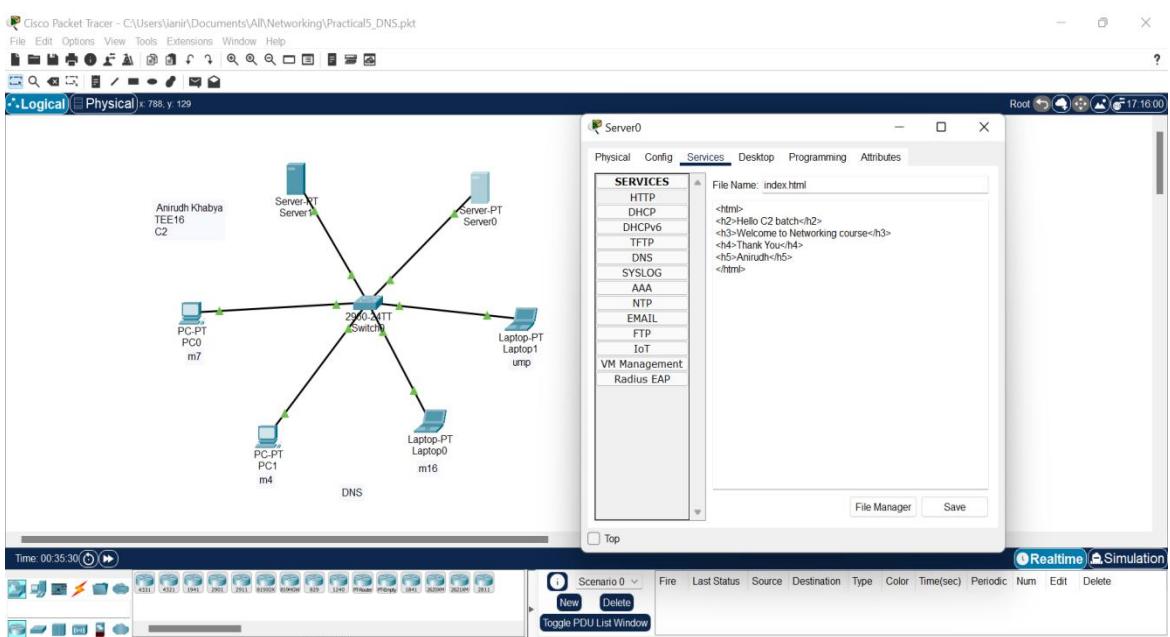
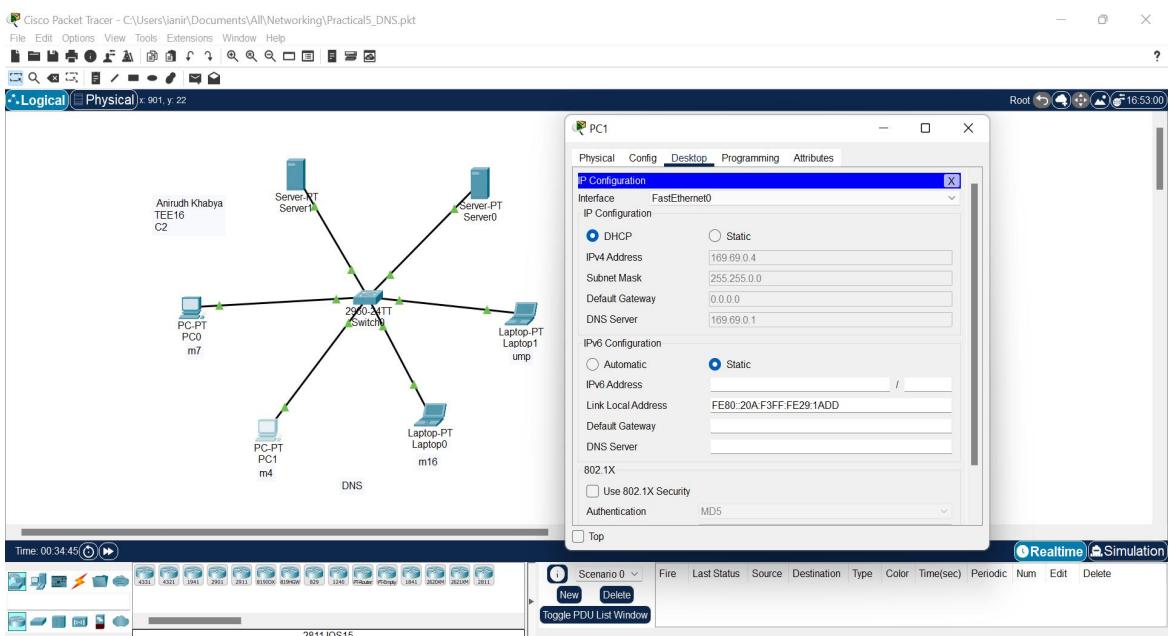
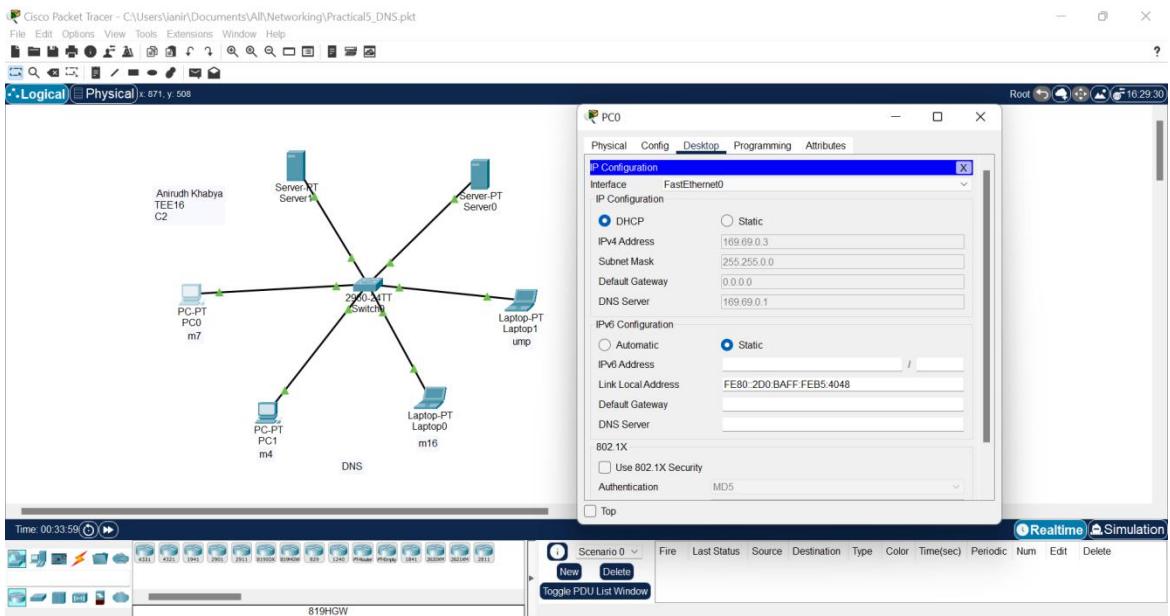
[A small page](#)
[Copyrights](#)
[Image page](#)
[Image](#)
[My First Web Page](#)

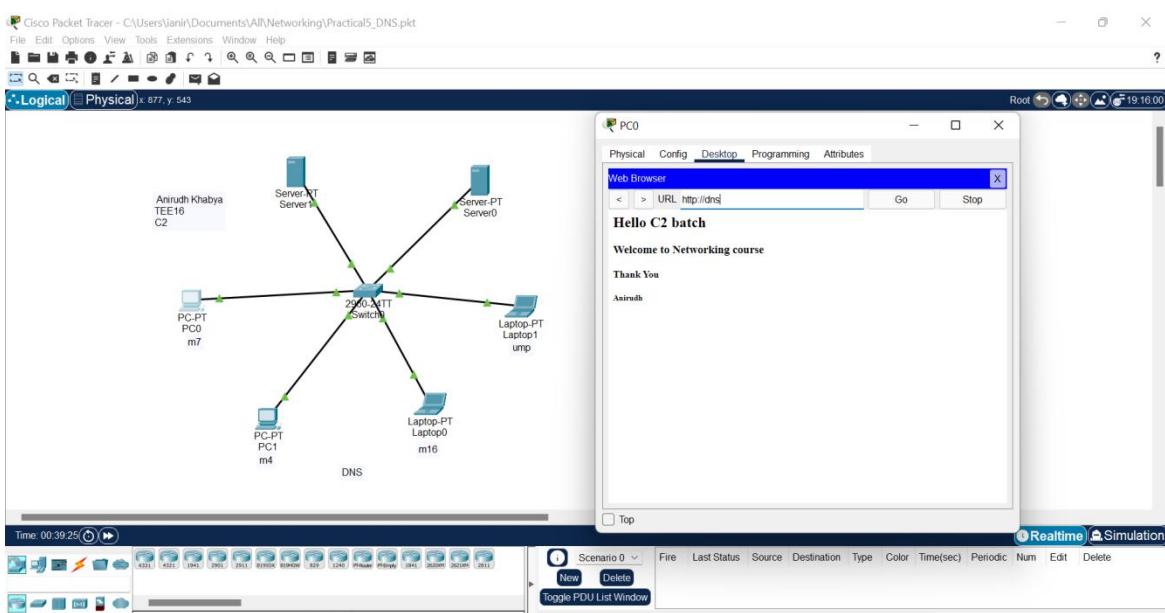
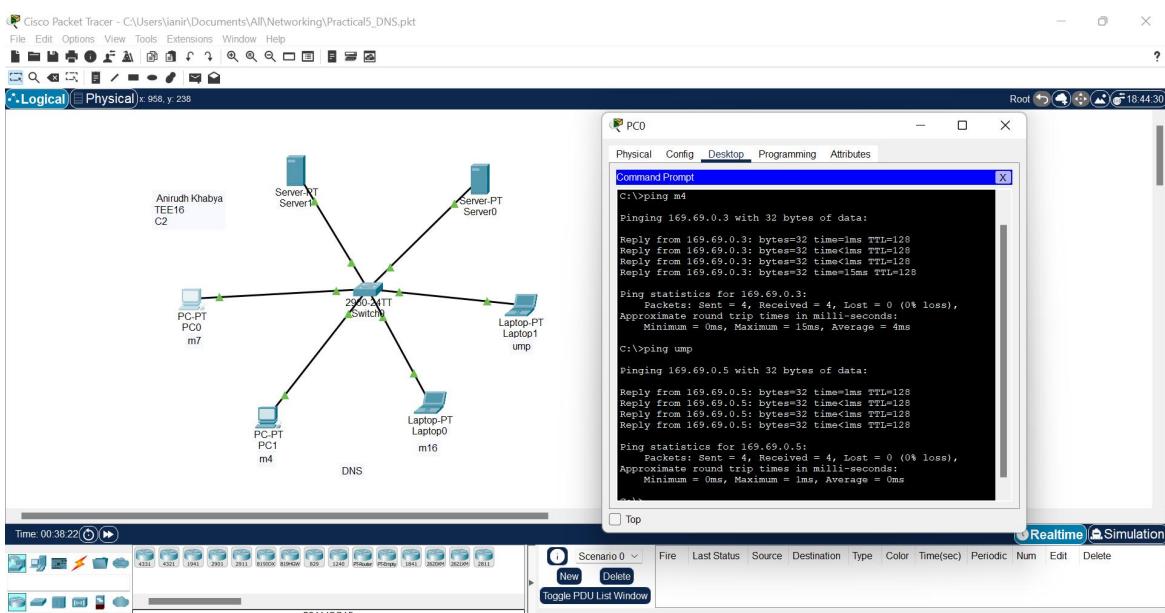
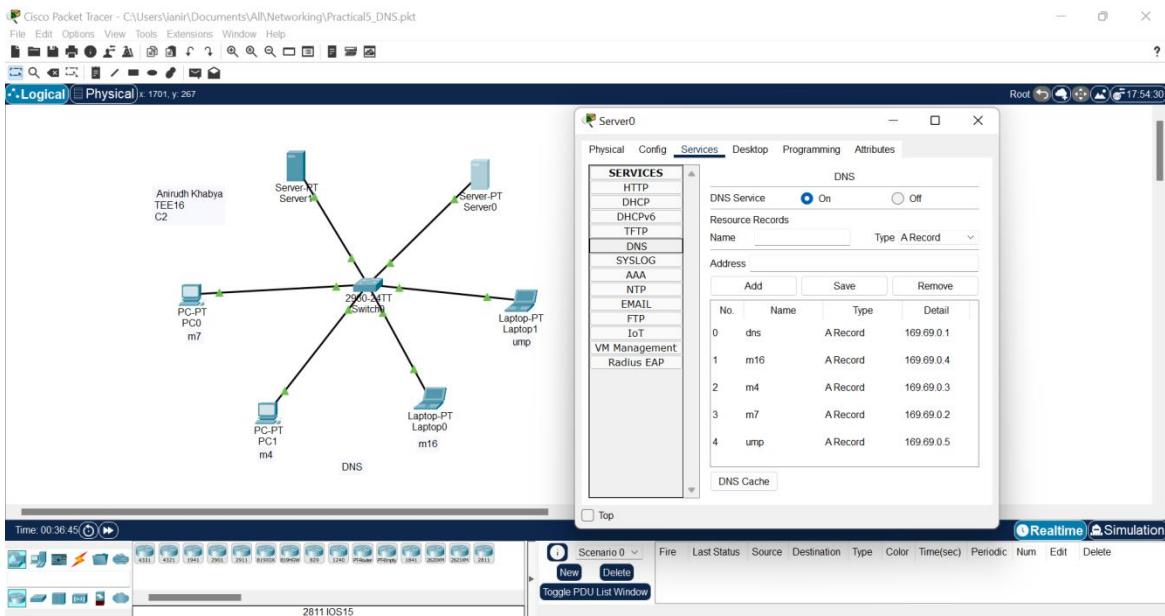
Just click on your page (My First Web Page)



Output







Conclusion:

In this experiment, we performed the configuration of network using application layers(DHCP, HTTP, DNS). The result of the experiment has successfully come.

Expt.No.7**Date:15/04/2022**

InstallationandconfigurationofTelnetserverforTelnetcommunication

Objective

- Telnet Configuration and Installation.
- Study different Telnet commands.
- Study communication between telnet client and server.

Requirements

- Personal computers with Network Interface Cards connected through category 5UTP cables.
- Windows 2000 Network Operating System installed in each computer.
- TCP/IP protocol installed in each computer.
- Students are provided with local administrator account.
- Mail boxes should be created on the Email server.

I. Introduction to Telnet

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-bandwidth with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol(TCP).

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol(TCP) port number 23, where a Telnet server application(telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program(NCP) protocols. When Telnet was initially developed in 1969, most users of networked computers

were in the computer departments of academic institutions, or at large private and government research facilities. In this environment, security was not nearly as much a concern as it became after the bandwidth explosion of the 1990s. The rise in the number of people with access to the Internet, and by extension the number of people attempting to hack other people's servers, made encrypted alternatives necessary. Experts in computer security, such as SANS Institute, recommend that the use of Telnet for remote login should be discontinued under all normal circumstances, for the following reasons: Telnet, by default, does not encrypt any data sent over the connection (including passwords), and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes; any body who has access to a router, switch, hub or gateway located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login, password and whatever else is typed with a packet analyzer. Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle. Several vulnerabilities have been discovered over the years in commonly used Telnet daemons. These security-related shortcomings have seen the usage of the Telnet protocol drop rapidly [citation needed], especially on the public Internet, in favor of the Secure Shell (SSH) protocol, first released in 1995. SSH provides much of the functionality of telnet, with the addition of strong encryption to prevent sensitive data such as passwords from being intercepted, and public key authentication, to ensure that the remote computer is actually who it claims to be. As has happened with other early Internet protocols, extensions to the Telnet protocol provide Transport Layer Security (TLS) security and Simple Authentication and Security Layer (SASL) authentication that address the above issues. However, most Telnet implementations do not support these extensions; and there has been relatively little interest in implementing these as SSH is adequate for most purposes. It is of note that there are a large number of industrial and scientific devices which have only Telnet available as a communication option. Some are built with only a standard RS-232 port and use a serial server hardware appliance to provide the translation between the TCP/Telnet data and the RS-232 serial data. In such cases, SSH is not an option unless the interface appliance can be configured for SSH.

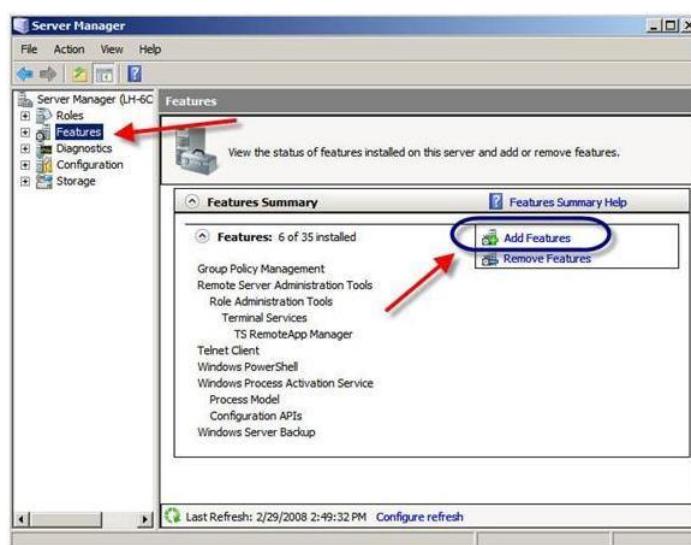
II. Installation and Configuration of Telnet Services

While the telnet client and server application has been around, well forever, it is still very useful and, if you are like me, you may use it every day for a variety of network configuration tasks. There are a number of reasons to configure a Windows

2000 Server as a Telnet server. Here is my list of them:

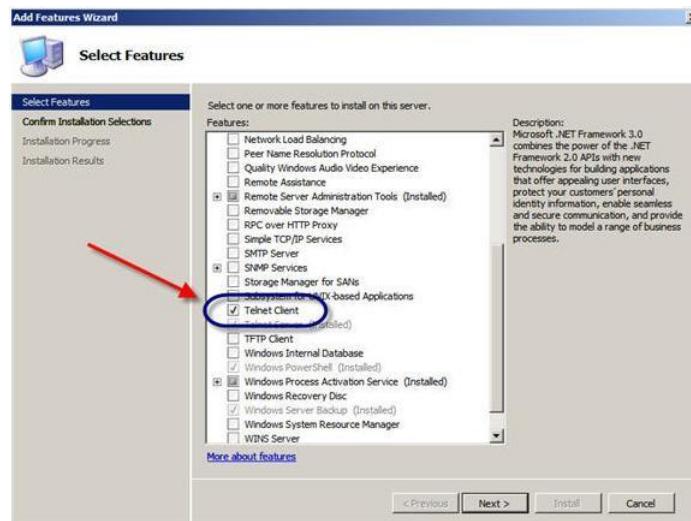
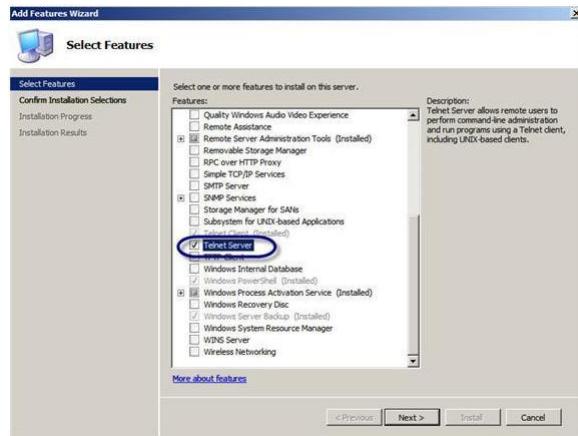
- To be able to configure and troubleshoot your network devices whether they are Cisco routers, Linux servers, or Windows 2008 Servers, from a quick and simple command line that is the Telnet application.
- To test connectivity to and from the server using a simple & reliable protocol

To install the Windows 2008 Server Telnet server, you need to add a new Windows Feature. To do this open up Server Manager and click on the Features section on the left. Next, click on Add Features on the right, like this:



On the Select Features window, scroll down to the Telnet Server option and click its check box to select it. Now, click Next, then Install.

This begins the installation of the Telnet Server. After a few minutes, you will get a message that the installation is complete. While, at this point, you could test your new Telnet Server from any computer that has the telnet application (like Windows XP or 2003) however, let's use a Windows Server with the telnet client to connect to your Windows Server that we just installed the Telnet server on. So, unlike in most previous Windows operating systems, we need to install the telnet client in Windows Server. To do this, we need to go into the same Server Manager application, to Features, then to Add Feature. This time, we will choose to install the Telnet Client, as shown below.

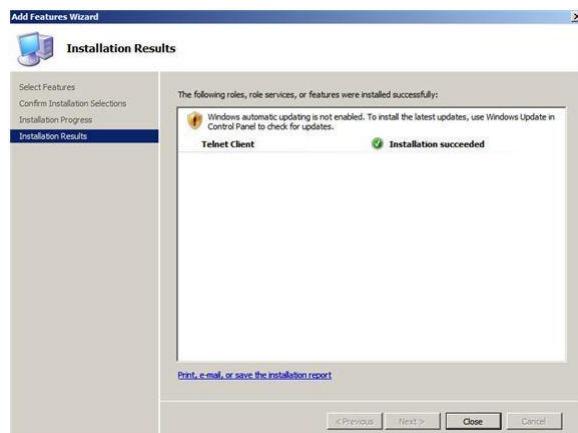


After clicking Next, then Install, my telnet client was installed very quickly, as you see in Figure, below.

Unlike many other features, just because the telnet server feature is installed, doesn't mean that it is working. To actually use the telnet server, you need to, minimally,

1) Start the service and 2) allow access. To start the service, go into the Services MMC either through the Start menu or by running services.msc. Change the telnet service to start automatically and then go ahead and Start the service.

To test connection, go to Start Command Prompt. At the Windows command prompt, telnet to new Telnet Server and check the ability to successfully connect, as a non-administrative user you can see below in Figure.



Services (Local)

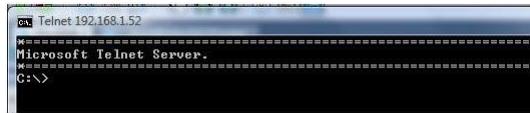
Telnet	Name	Description	Status	Startup Type	Log On As
Stop the service	System Event Notif...	Monitors s...	Started	Automatic	Local System
Pause the service	Task Scheduler	Enables a ...	Started	Automatic	Local System
Restart the service	TCP/IP NetBIOS He...	Provides s...	Started	Automatic	Local Service
	Telephony	Provides t...	Manual		Network a...
	Telnet	Enables a r...	Started	Automatic	Local Service

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\David>telnet 192.168.1.52
```

```
C:\> Telnet 192.168.1.52
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+J'

You are about to send your password information to a remote computer in zone. This might not be safe. Do you want to send anyway(y/n): y
```

```
C:\> Telnet 192.168.1.52
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password
Welcome to Microsoft Telnet Service
Login: ddavis
password:
```



The two important things of note that can be learnt from the above Figures are;

- Per the warning message above in Figures, Telnet is an insecure protocol. All traffic sent (including your username & password) are send in clear text across the network. That means that your username & password could be seen by some one who is decoding packets on your network. This is a security risk even on a secure internal LAN.
- However from Figure, Windows Telnet supports NTLM authentication. You can force the telnet server to only allow NTLM authentication and this would make your telnet server much more secure.

Additionally, after reading the official Microsoft telnet operations guide below, we can learn how to customize the configuration for telnet and do things such as change the port number used, idle time, max # of simultaneous users, and more. To see who is connected to your telnet server, following command can be used:

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>telntadm -s
1 telnet session(s)

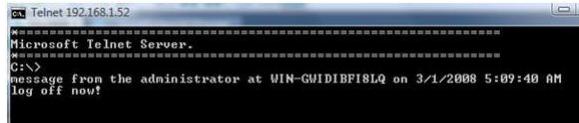
ID Domain UserName Client LogonDate LogonTime
IdleTime (hh:mm:ss)
-----
2068 WIN-GWJ1IBFI8LQ ddavis ::ffff:192.168.1.182 3/1/2008 4:59:21 AM
0:09:20

C:\Users\Administrator>
```

Also, other functions can be done with the `telntadm` command like send messages to users (below, in Figure) and disconnect users.

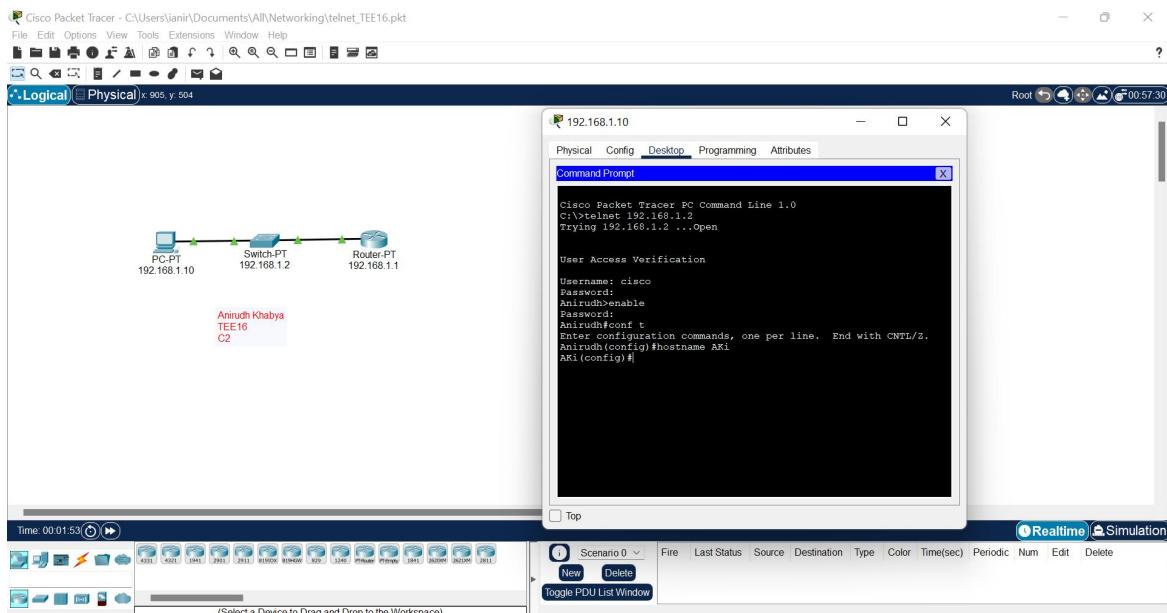
```
C:\Users\Administrator>telntadm -m all "log off now!"
The message sent successfully.

C:\Users\Administrator>
```



There are a lot of benefits to adding a Telnet Server to your Windows Server system. We learned that there is more to using the telnet server than just installing the feature. The telnet server has to be started and user authentication has to be configured before the telnet server can be used. The telnet server can be used for many different types of command line administration, monitoring, and troubleshooting of your Windows Server.

Results:



Conclusion:

In this lab session, we have performed the experiment on telnet. It enables you to set up TCP/IP connections to a host. Telnet allows a person at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

Expt.No.8**Date:15/04/2022**

Configure network using Distance Vector Routing Protocol

Objective

- To configure network using Distance Vector Routing Protocol

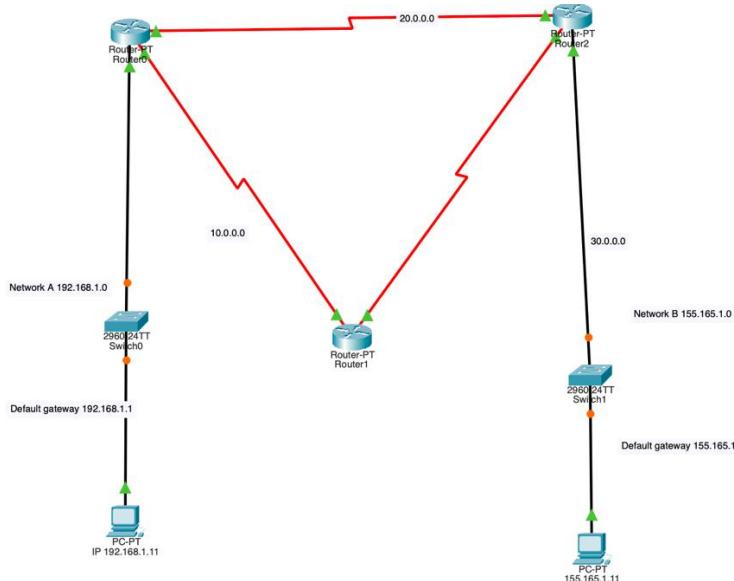
Requirements

- CCNA Packet Tracer

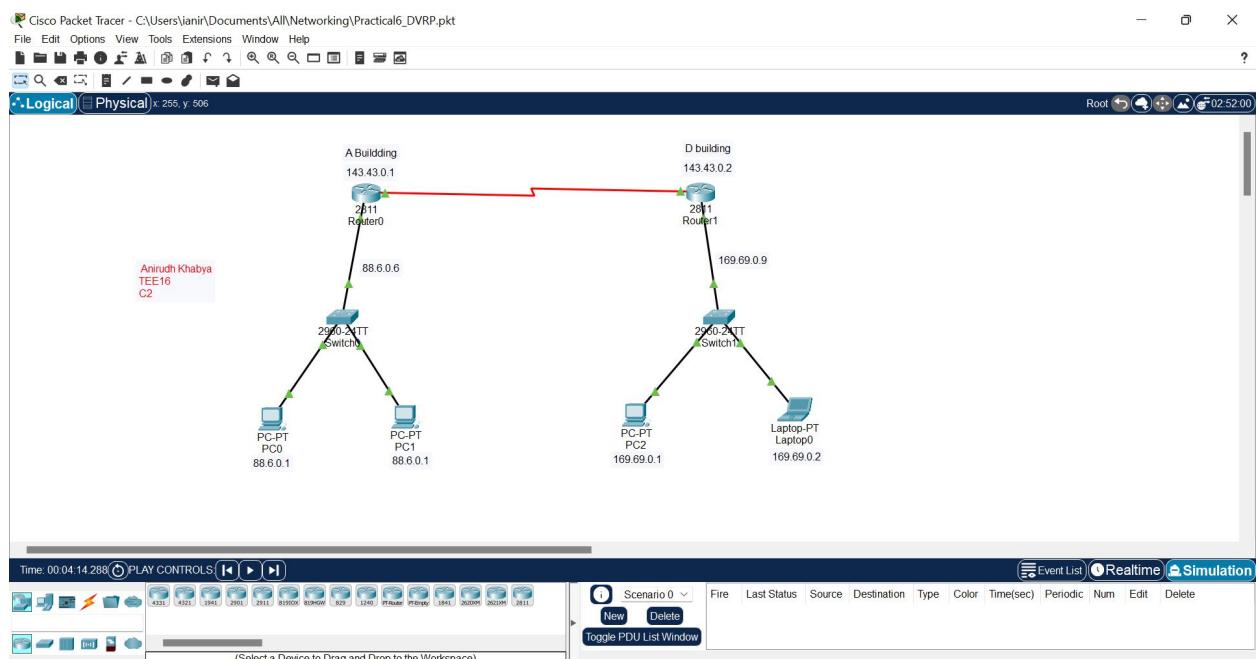
Theory:

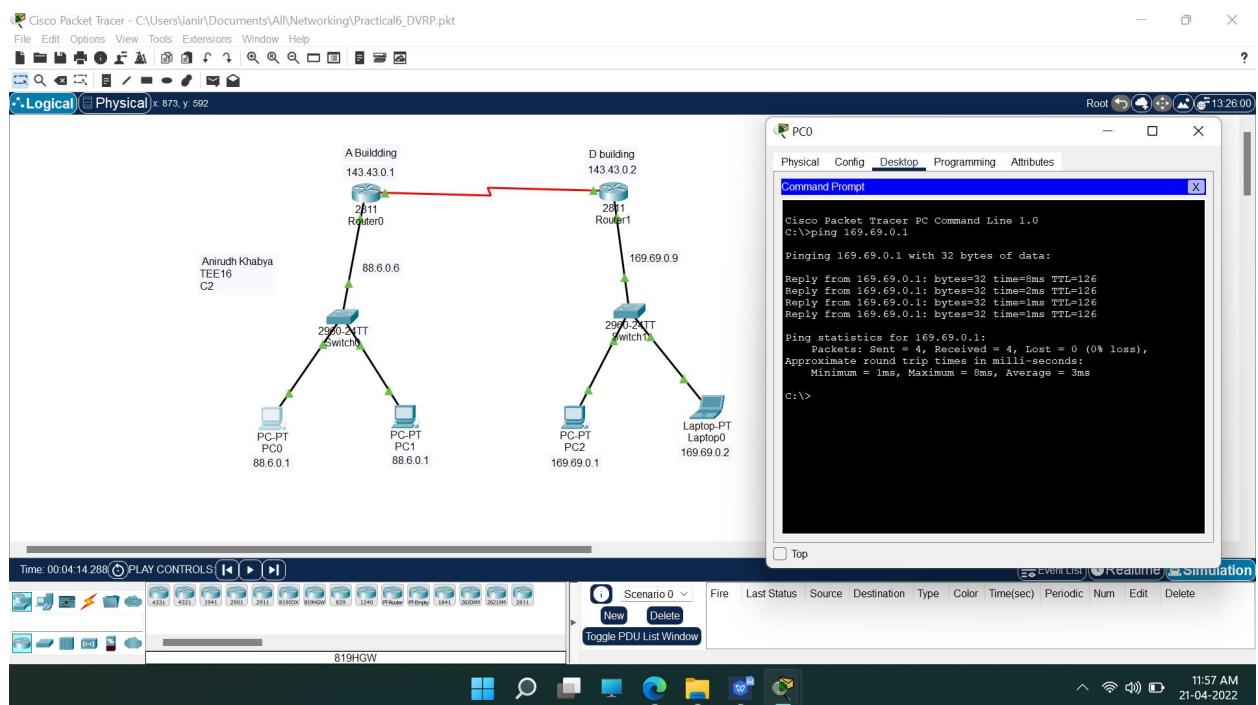
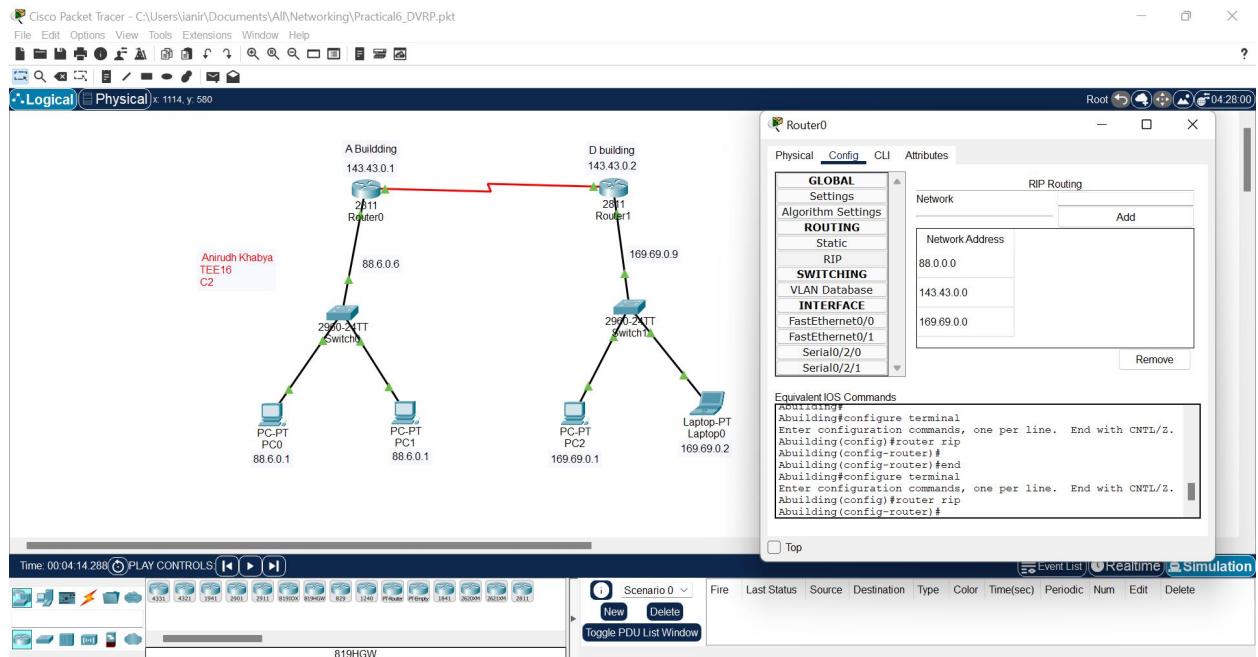
Distance Vector Routing Protocol

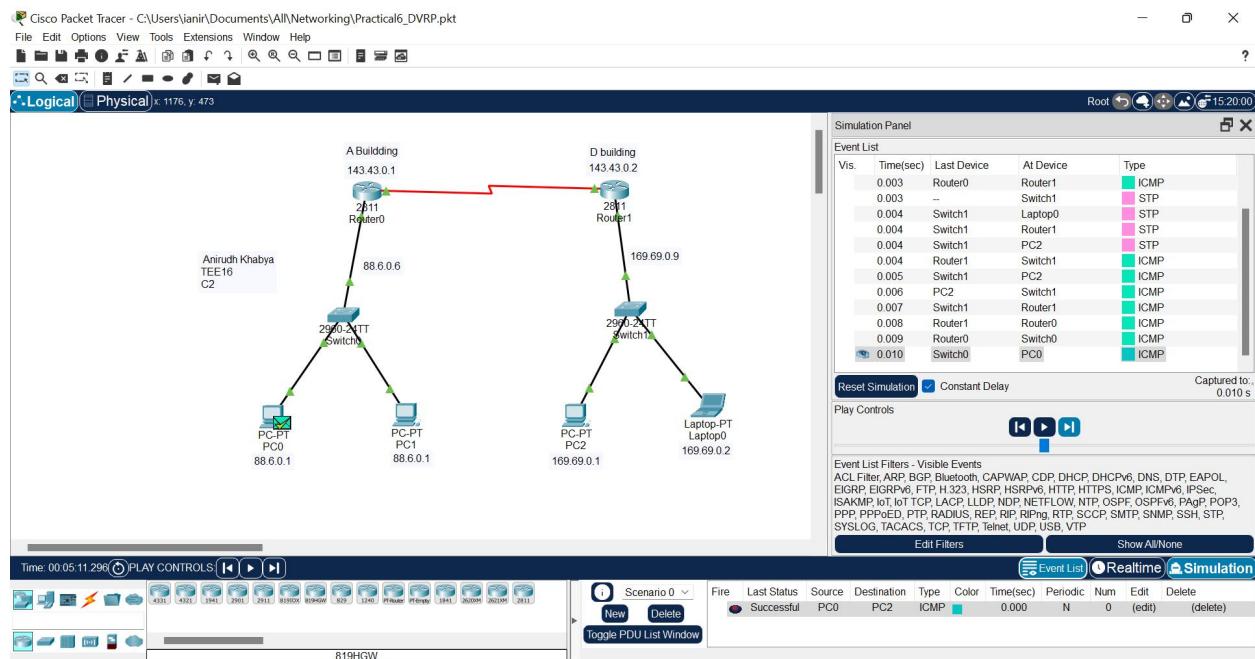
- A distance-vector routing protocol in data networks determines the best route for data packets based on distance
- Measure the distance by the number of routers a packet has to pass, one router counts as one hop
- Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route
- Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances, based on a chosen metric, are computed using information from the neighbours' distance vectors
- A router transmits its distance vector to each of its neighbours in a routing packet
- Each router receives and saves the most recently received distance vector from each of its neighbour
- A router recalculates its distance vector when:
- It receives a distance vector from a neighbour containing different information than before.
- It discovers that a link to a neighbour has gone down
- The DV calculation is based on minimizing the cost to each destination



Result:







Conclusion:

In this lab session, we have done the experiment on DVRP(Distance Vector Routing Protocol). It share, the information of the entire autonomous system and the information is shared only with neighbour. On the other hand, in link state the routers share the knowledge only about their neighbour and the information is shared with all routers.

Expt.No.9**Date:15/04/2022**

Linked State Routing Protocol

Objective

- To configure network using Linked State Routing Protocol

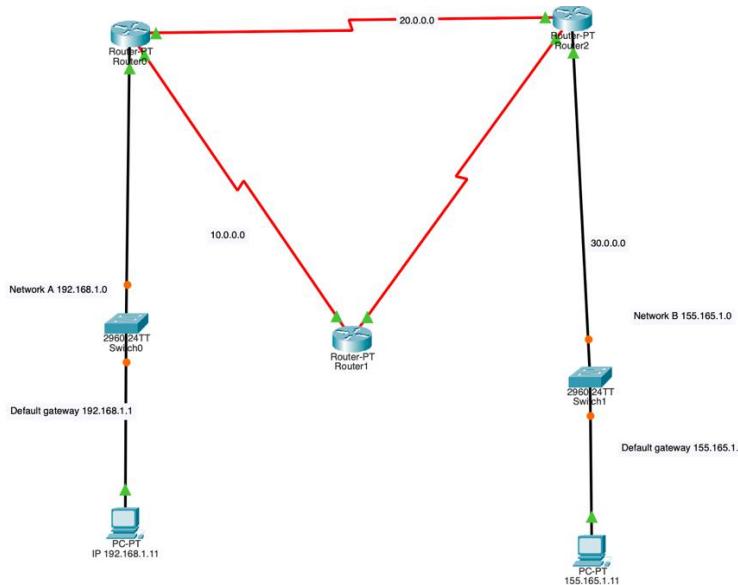
Requirements

- CCNA Packet Tracer

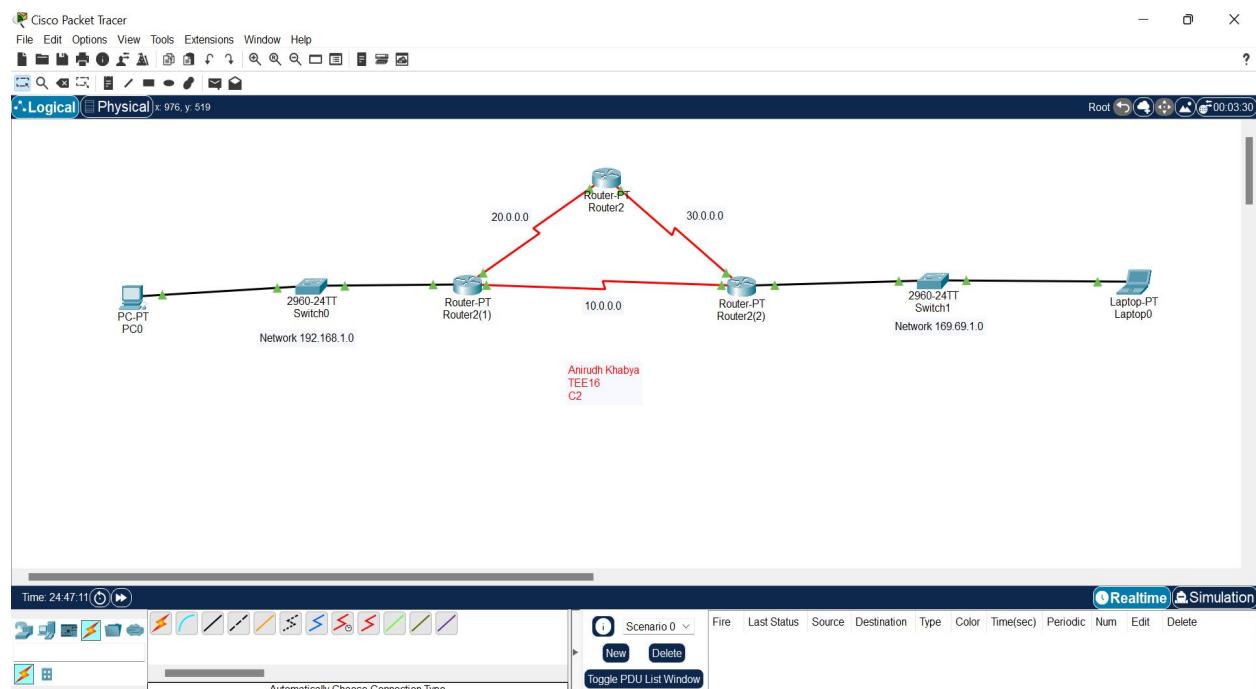
Theory:

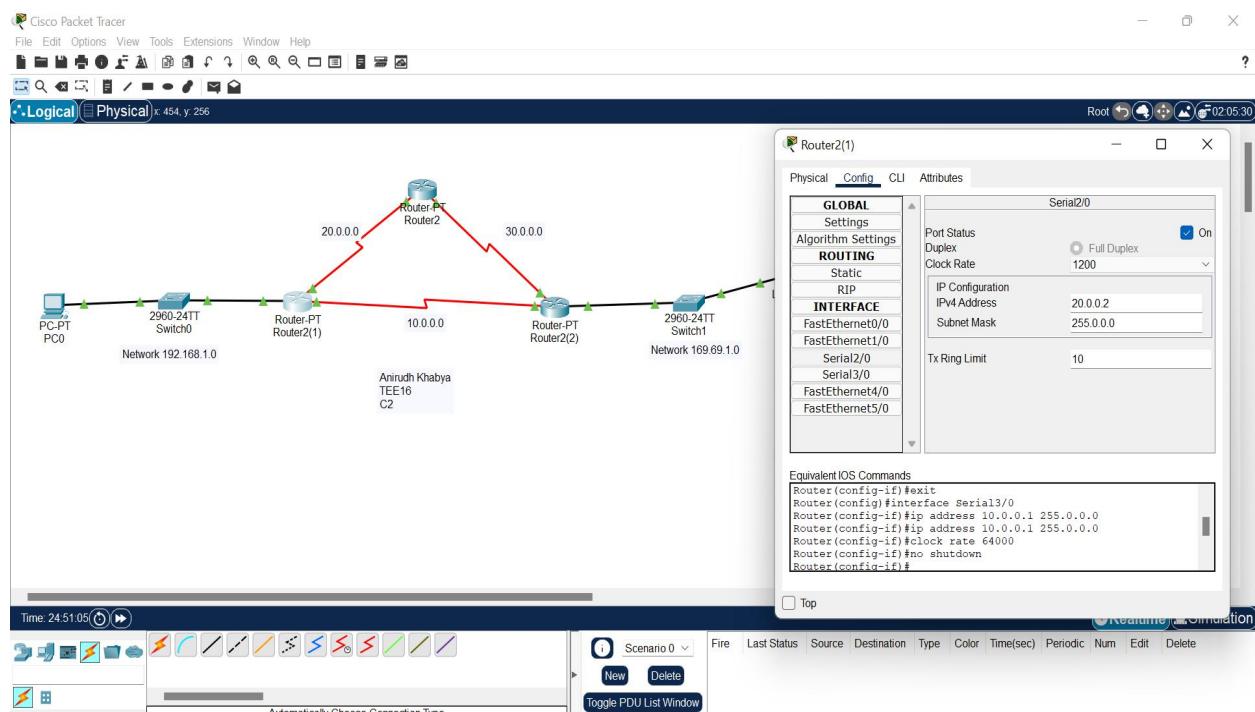
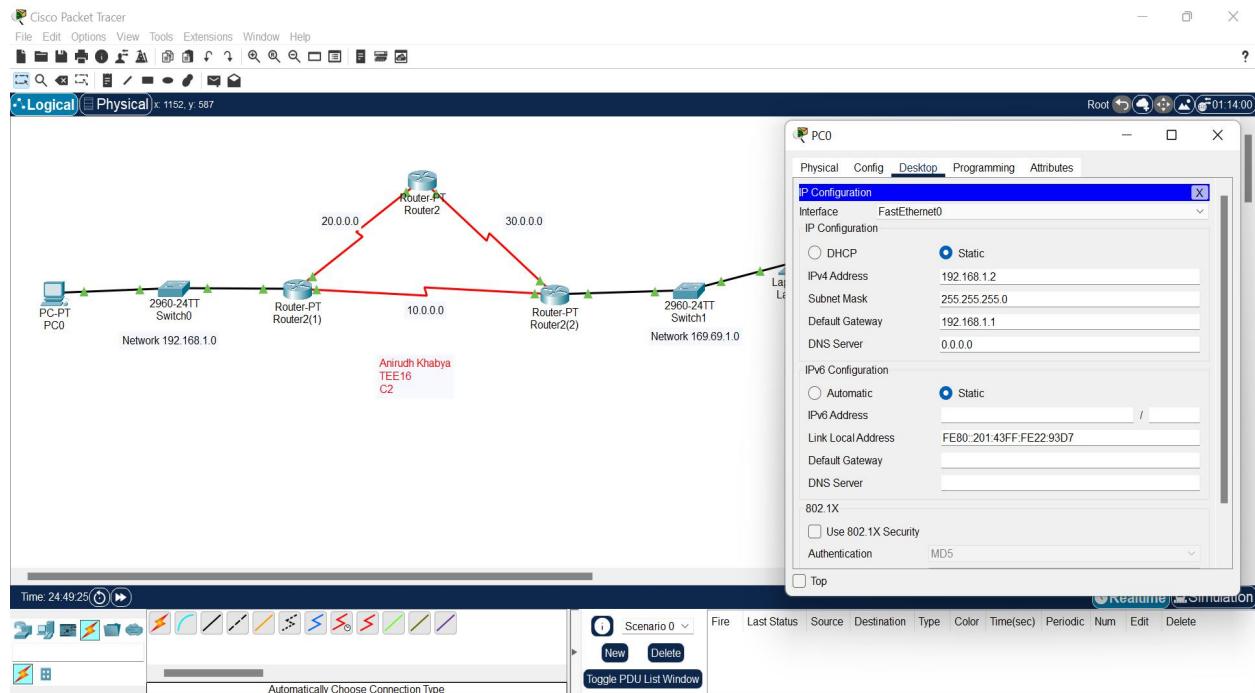
Distance Vector Routing Protocol

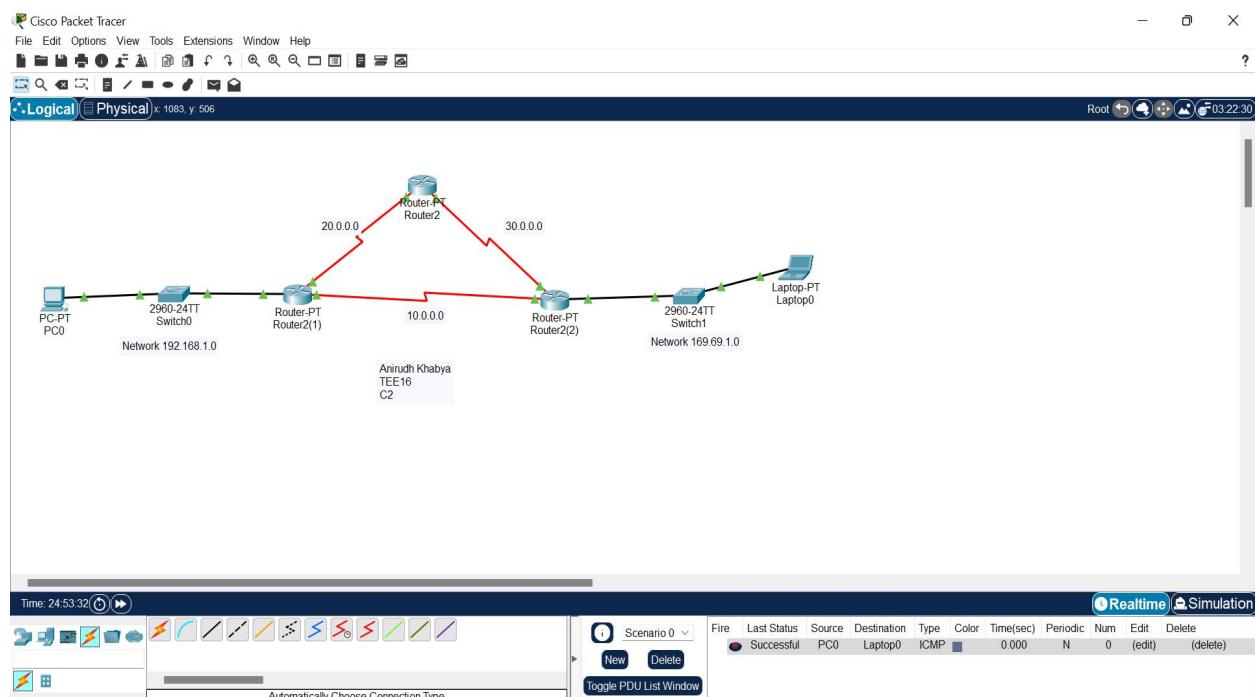
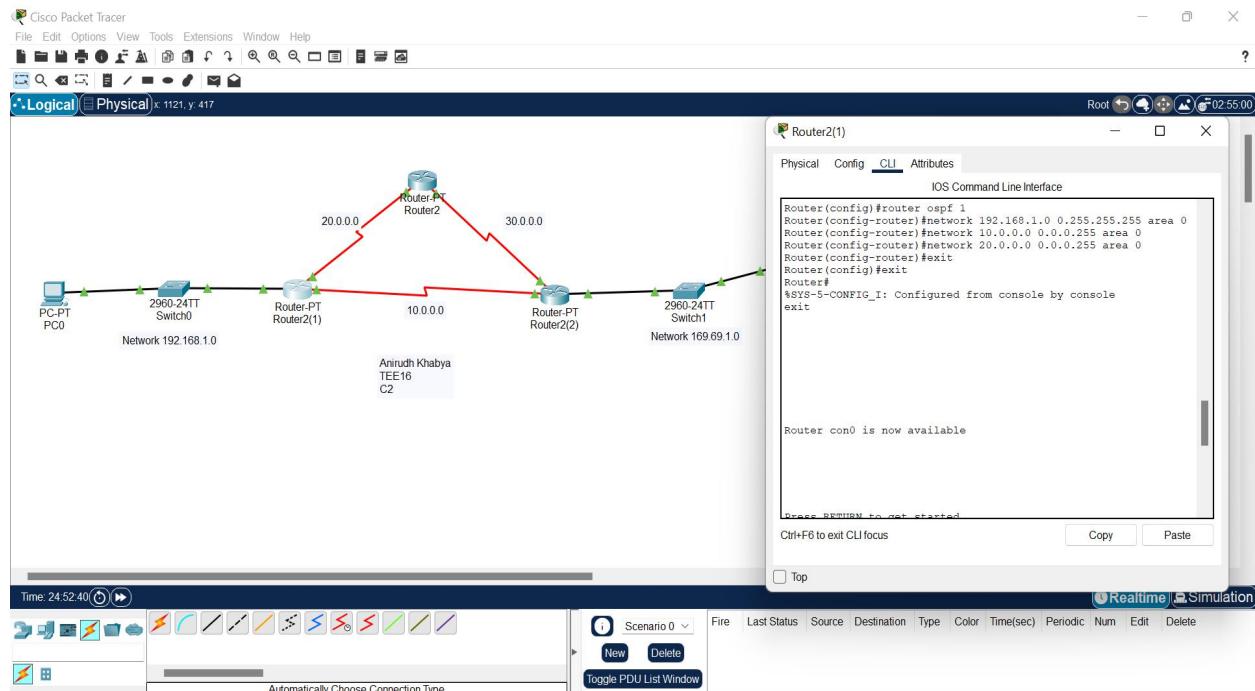
- A distance-vector routing protocol in data networks determines the best route for data packets based on distance
- Measure the distance by the number of routers a packet has to pass, one router counts as one hop
- Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route
- Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances, based on a chosen metric, are computed using information from the neighbours' distance vectors
- A router transmits its distance vector to each of its neighbours in a routing packet
- Each router receives and saves the most recently received distance vector from each of its neighbours
- A router recalculates its distance vector when:
 - It receives a distance vector from a neighbour containing different information than before.
 - It discovers that a link to a neighbour has gone down
 - The DV calculation is based on minimizing the cost to each destination

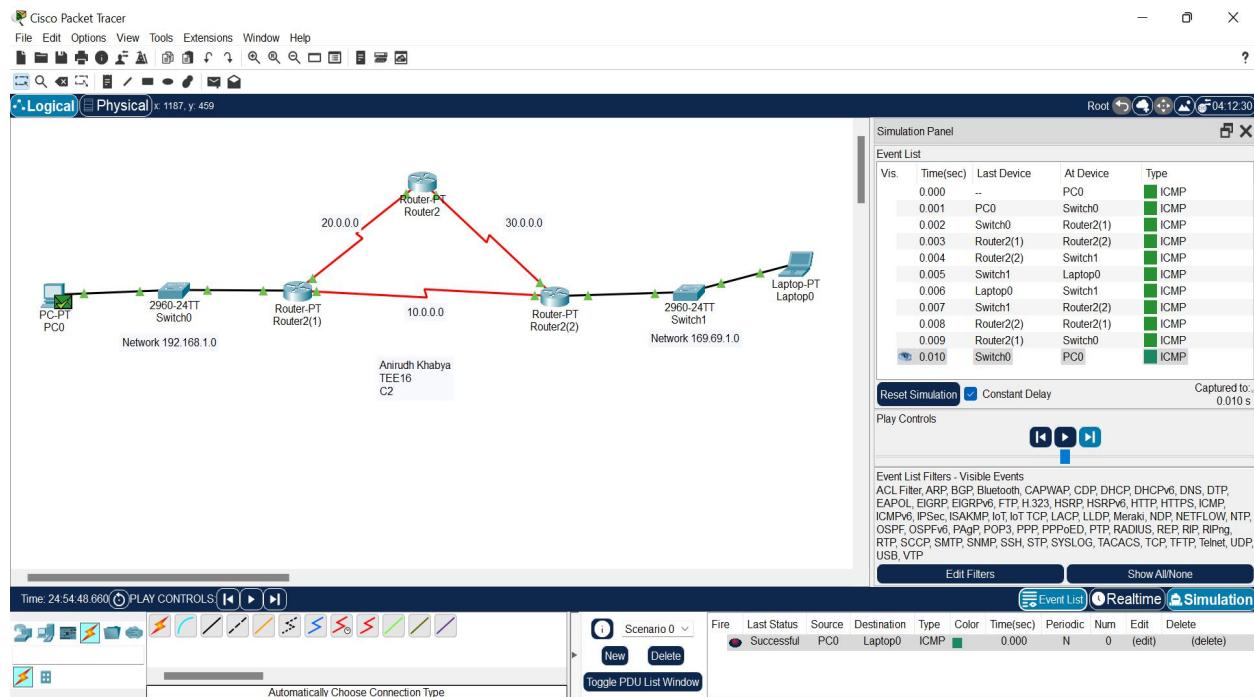


Results:









Conclusion:

In this lab session, we have configured network using linked state vector routing protocol. Link State Packet (LSP) is a packet of information generated by a network router in a link state routing protocol that lists the router's neighbors. Link state packet can also be further defined as special datagrams that determine the names of and the cost or distance to any neighboring routers and associated networks.