

Vaagdevi College of Engineering

Department of Computer Science and Engineering



B.Tech III year I Semester

Computer Networks Lab Manual



S.No	Experiment
Week 1	Study of different types of Network cables and practically implement the cross-wired cable and straight through cable using clamping tool.
Week 2	Study of Network Devices in Detail.
Week 3	Study of network IP.
Week 4	Connect the computers in Local Area Network.
Week 5	Study of basic network command and Network configuration commands.
Week 6	Configure Star topology using packet tracer software.
Week 7	Configure Bus topology using packet tracer software.
Week 8	Configure Mesh topology using packet tracer software.

Hardware and Software Requirement

Hardware Requirement

RJ-45 connector, Crimping Tool, Twisted pair Cable, 160 GB hard disk , Dual core processor, 2 GB RAM

Software Requirement

Command Prompt and CISCO Packet Tracer, JAVA latest version.

EXPERIMENT-1

Aim: Study of different types of Network cables and practically implement the cross-wired cable and straight through cable using clamping tool.

Apparatus (Components): RJ-45 connector, Clipping Tool, Twisted pair Cable

Procedure: To do these practical following steps should be done:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very 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.


2. 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.

3. 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 Cross wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Diagram shows you how to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

EXPERIMENT-2

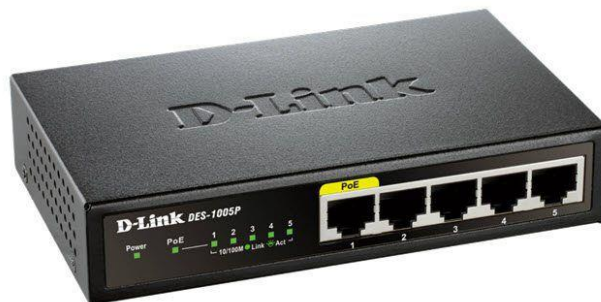
Aim: Study of Network Devices in Detail

- Repeater
- Hub
- Switch
- Bridge
- Router
- Gate Way

Apparatus (Software): No software or hardware needed.

Procedure: Following should be done to understand this practical.

1. **Repeater:** Functioning at Physical Layer. A **repeater** is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports ,so cannot be use to connect for more than two devices
2. **Hub:** Hub is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.



There are two types of the Hub.

Passive Hub: - It forwards data signals in the same format in which it receives them. It does not change the data signal in any manner.

Active Hub: - It also works same as the passive Hub works. But before forwarding the data signals, it amplifies them. Due to this added feature, the active Hub is also known as the repeater.

3. **Switch:** A **network switch** or **switching hub** is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.



- A switch manages the flow of data across a network by inspecting the incoming frame's destination MAC address and forwarding the frame only to the host for which the data was intended.
- Each switch has a dynamic table (called the MAC address table) that maps MAC addresses to ports. With this information, a switch can identify which system is sitting on which port and where to send the received frame.

4. **Bridge:** A **network bridge** connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term *bridge* formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. *Switch* or *Layer 2 switch* is often used interchangeably with *bridge*. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.



There are three types of Bridge:-

Local Bridge: - This Bridge connects two LAN segments directly. In Ethernet Implementation, it is known as the **Transparent Bridge**.

Remote Bridge: - This Bridge connects with another Bridge over the WAN link.

- It is also called as Translational Bridge.

Wireless Bridge: - A wireless bridge is a type of networking hardware device that enables the connection of two different local area network (LAN) segments by bridging a wireless connection between them.

5. **Router:** A **router** is an electronic device that interconnects two or more computer networks,

and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.



6. **Gate Way:** In a communications network, a network node equipped for interfacing with another network that uses different protocols.

- A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.
- A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

EXPERIMENT- 3**Aim:** Study of Network IP

- Classification of IP address
- Sub netting
- Super netting

Apparatus (Software): NA**Procedure:** Following is required to be study under this practical.

- Classification of IP address

IP address

Every device that connects to the Internet is assigned a unique IP (Internet Protocol) address, enabling data sent over the Internet to reach the right device out of the billions of devices connected to the Internet. While computers read IP addresses as binary code (a series of 1s and 0s), IP addresses are usually written as a series of alphanumeric characters.

TCP/IP defines five classes of IP addresses: class A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the class. IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes – class D for multicast and class E for experimental purposes.

The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size.

As show in figure we teach how the ip addresses are classified and when they are used.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

Sub netting

Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network.

Super netting

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernet or Supernet.

EXPERIMENT-4

Aim: Connect the computers in Local Area Network.

Procedure: On the host computer

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Network Connections**.
5. Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.
6. Click **Properties**.
7. Click the **Advanced** tab.
8. Under **Internet Connection Sharing**, select the **Allow other network users to connect through this computer's Internet connection** check box.
9. If you are sharing a dial-up Internet connection, select the **Establish a dial-up connection whenever a computer on my network attempts to access the Internet** check box if you want to permit your computer to automatically connect to the Internet.
10. Click **OK**. You receive the following message:

When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

11. Click **Yes**.

The connection to the Internet is shared to other computers on the local area network (LAN).

The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0.1 and a subnet mask of 255.255.255.0

On the client computer

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer. To confirm the LAN adapter IP configuration, follow these steps:

1. Log on to the client computer as Administrator or as Owner.

2. Click **Start**, and then click **Control Panel**.
 3. Click **Network and Internet Connections**.
 4. Click **Network Connections**.
 5. Right-click **Local Area Connection** and then click **Properties**.
 6. Click the **General** tab, click **Internet Protocol (TCP/IP)** in the **connection uses the following items** list, and then click **Properties**.
 7. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Obtain an IP address automatically** (if it is not already selected), and then click **OK**.
- Note:** You can also assign a unique static IP address in the range of 192.168.0.2 to 192.168.0.254. For example, you can assign the following static IP address, subnet mask, and default gateway:
8. IP Address 192.168.31.202
 9. Subnet mask 255.255.255.0
 10. Default gateway 192.168.31.1
11. In the **Local Area Connection Properties** dialog box, click **OK**.
 12. Quit Control Panel.

EXPERIMENT- 5

Aim: Study of basic network command and Network configuration commands.

Apparatus (Software): 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.

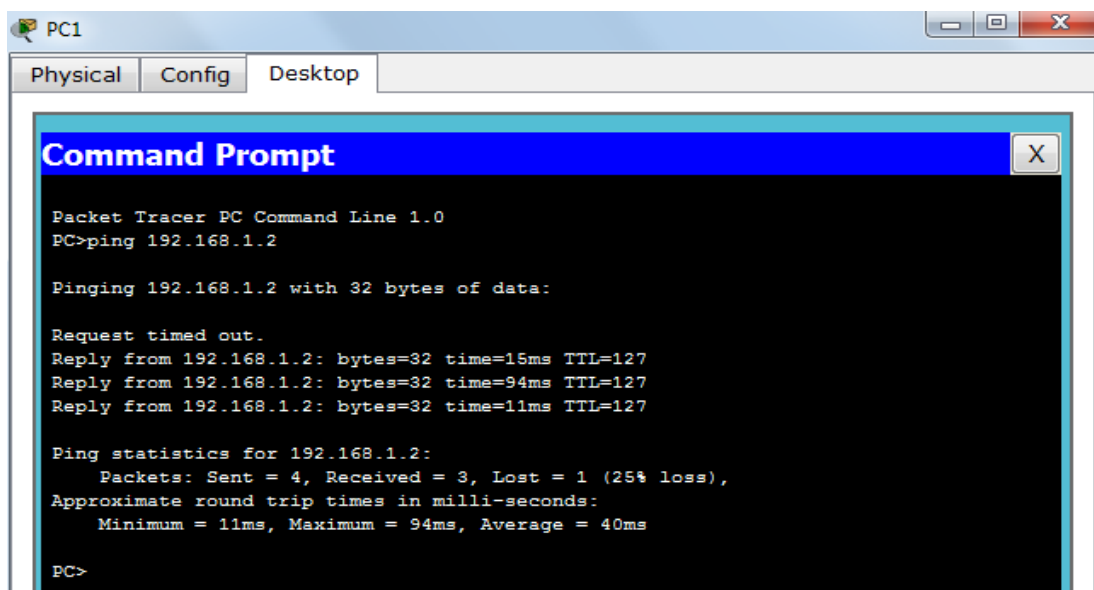
All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

This 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.



The screenshot shows a Packet Tracer PC window titled 'PC1' with tabs for 'Physical', 'Config', and 'Desktop'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The Command Prompt shows the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

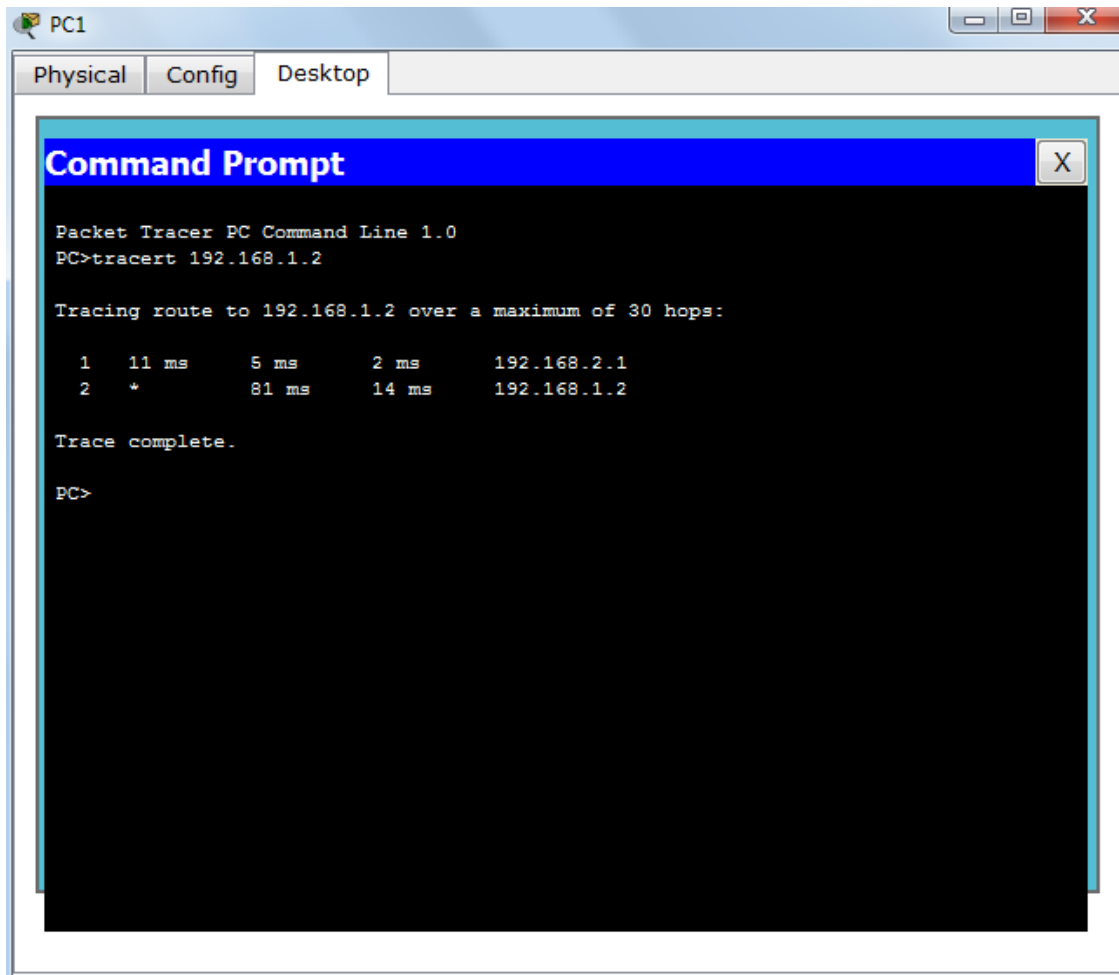
Request timed out.
Reply from 192.168.1.2: bytes=32 time=15ms TTL=127
Reply from 192.168.1.2: bytes=32 time=94ms TTL=127
Reply from 192.168.1.2: bytes=32 time=11ms TTL=127

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>
```

Traceroute:

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.



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 statistics about packet loss and latency.

```
Administrator: C:\windows\system32\cmd.exe

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 [192.168.1.97]
  1  lenovo-PC.dronacharya [192.168.1.97]  reports: Destination host unreachable
.

Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
   0  ---      Lost/Sent = Pct  Lost/Sent = Pct  lenovo-PC.dronacharya [192.168.1.97]
   1  ---      100/ 100 =100%   100/ 100 =100%   ! lenovo-PC [0.0.0.0]

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 startup configuration.

Use the following privileged mode commands to work with configuration files.

- **configure terminal** – modify the running configuration manually from the terminal.
- **show running-config** – display the running configuration.
- **show startup-config** – display the startup configuration.
- **copy running-config startup-config** – copy the running configuration to the startup configuration.
- **copy startup-config running-config** – copy the startup configuration to the running configuration.
- **erase startup-config** – erase the startup-configuration in NVRAM.
- **copy tftp running-config** – load a configuration file stored on a Trivial File Transfer Protocol (TFTP) server into the running configuration.
- **copy running-config tftp** – store the running configuration on a TFTP server.

IP Address Configuration

Take the following steps to configure the IP address of an interface. Step 1: Enter privileged EXEC mode:

Router>**enable** password

Step 2: Enter the **configure terminal** command to enter global configuration mode. Router#**config terminal**

Step 3: Enter the **interface** type slot/port (for Cisco 7000 series) or **interface** type port (for Cisco 2500 series) to enter the interface configuration mode.

Example:

Router (config)#**interface ethernet 0/1**

Step 4: Enter the IP address and subnet mask of the interface using the **ip address** ipaddress subnetmask command.

Example,

Router (config-if)#**ip address 192.168.10.1 255.255.255.0**

Step 5: Exit the configuration mode by pressing Ctrl-Z Router(config-if)#**[Ctrl-Z]**

EXPERIMENT-6

Aim: Configure Star topology using packet tracer software.

Apparatus (Software): Packet tracer Software

Procedure: To implement this practical following network topology is required to be configured using following steps.

Star Topology:

Star topology is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card used in each computer of the star topology, a coaxial cable or an RJ-45 network cable is used to connect computers together.



Advantages of star topology

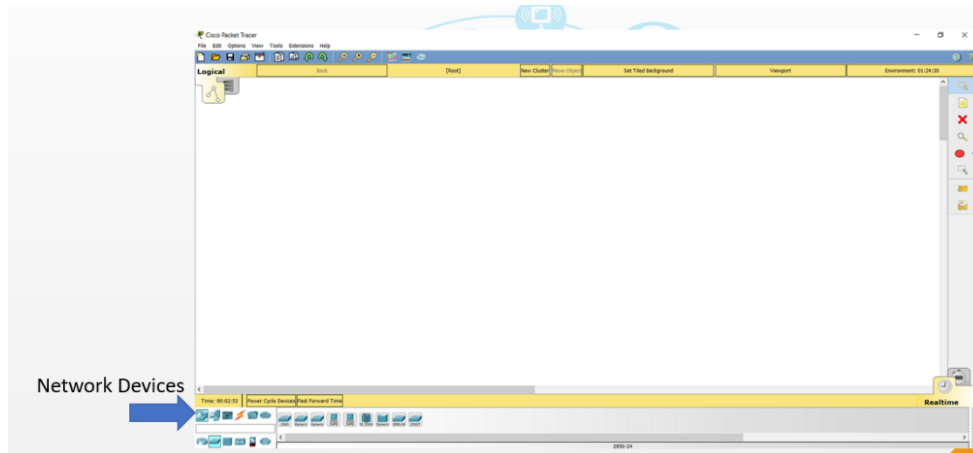
- Centralized management of the network, through the use of the central computer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.

Disadvantages of star topology

- May have a higher cost to implement.
- The central network device determines the performance and number of nodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network.

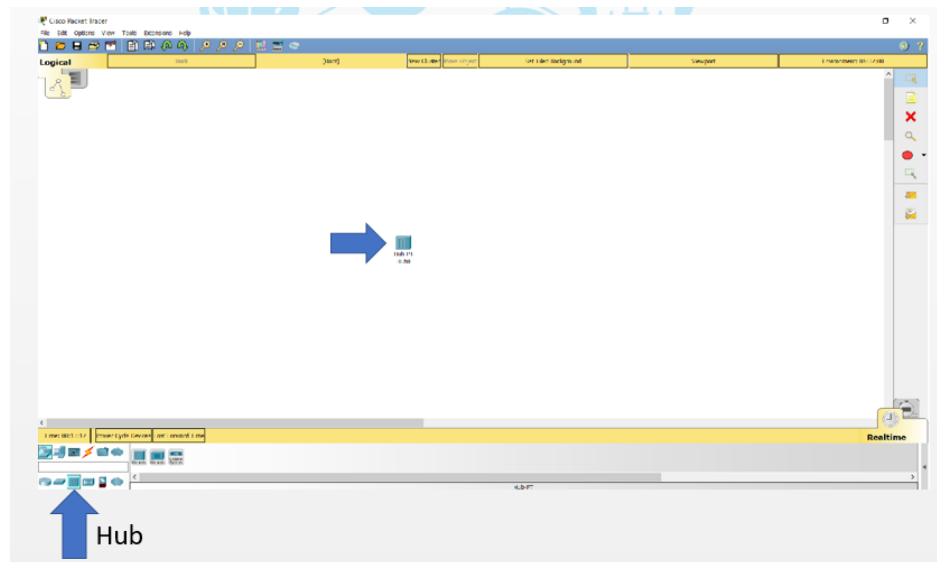
Step 1:

- Open Cisco Packet Tracer and Open Networking Device Menu.



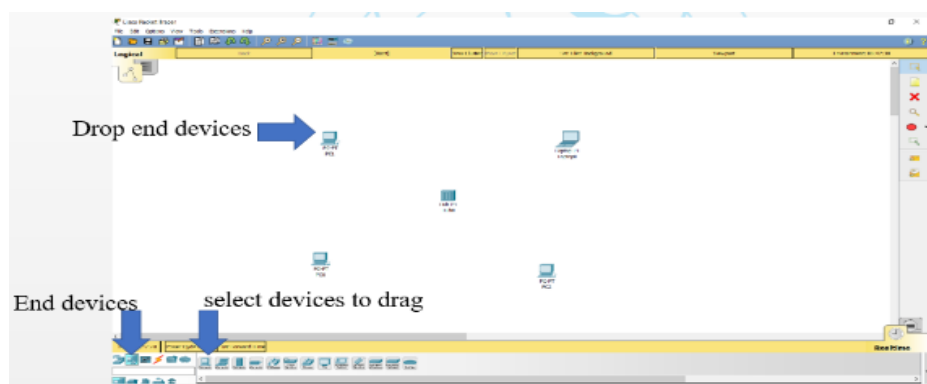
Step 2:

- Select Hub and drag it onto the work area.



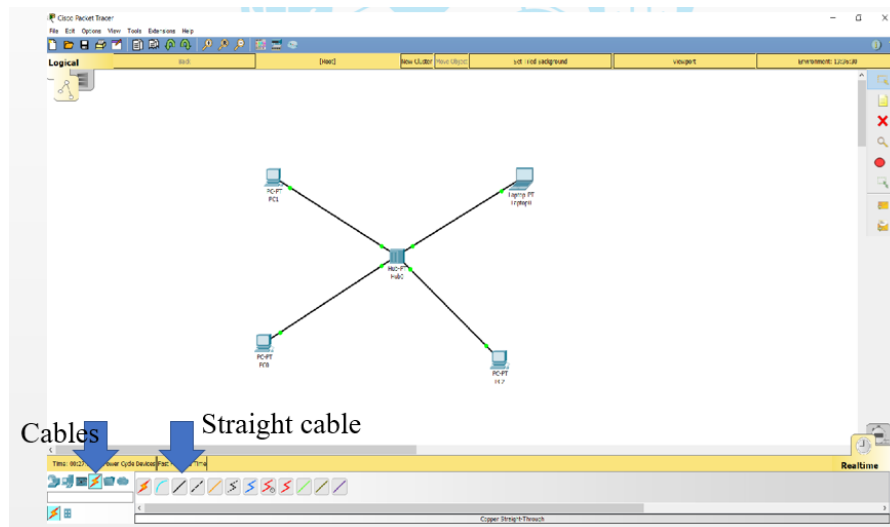
Step 3:

- Click on End Devices and select an end device.
- Drag selected end device to the work area.

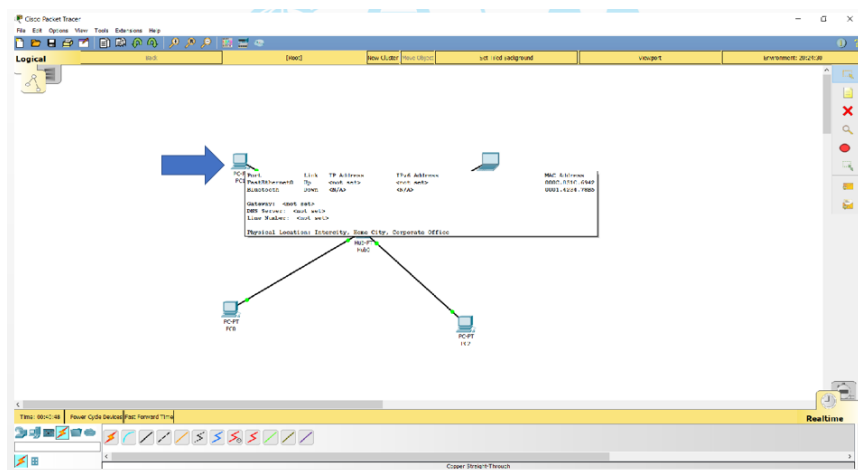


Step 4:

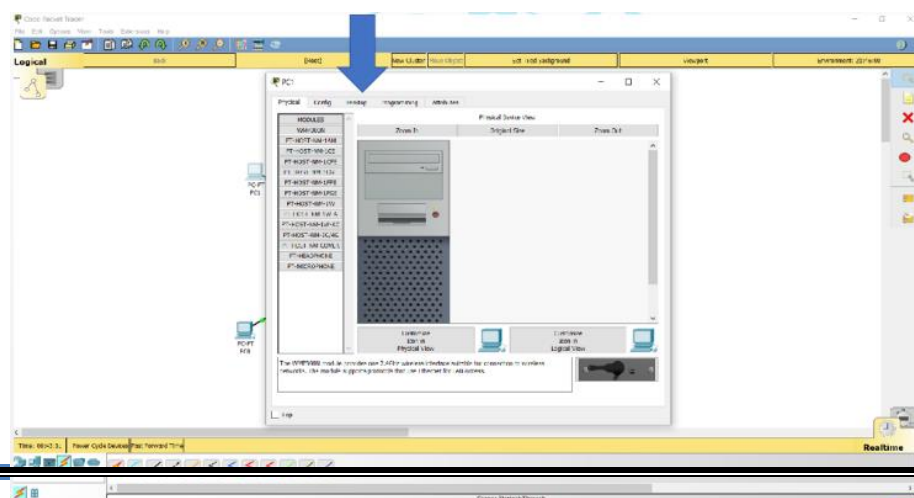
- Choose Connecting Cable for Device Connections
- Click on cables and select straight through cable
- Connect end devices to hub.



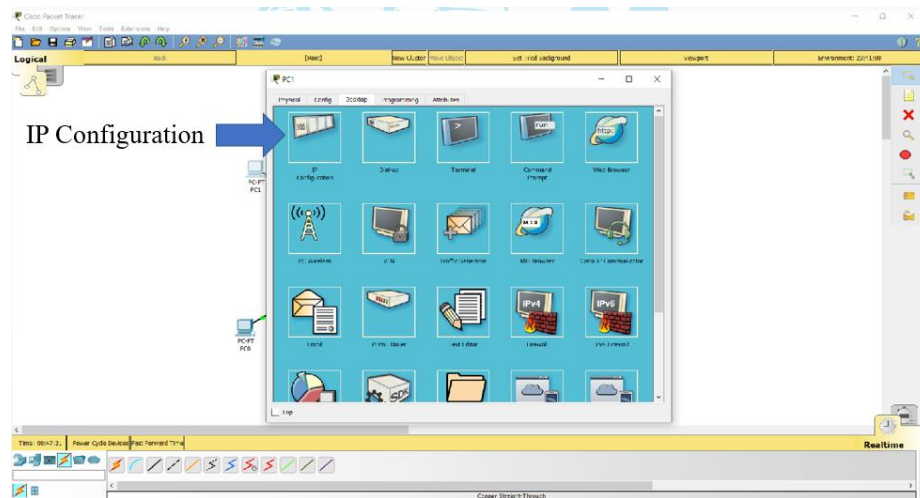
Step 5: Configure IP Address and Subnet Mask



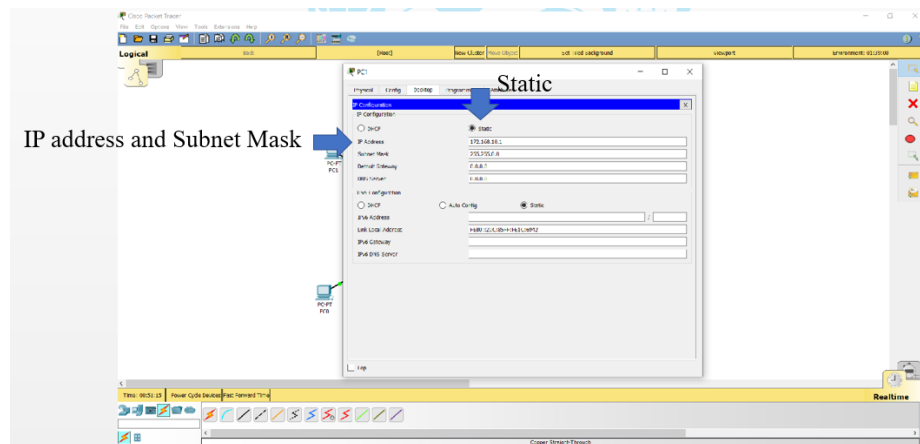
- Once you click on end device it displays the below window, here you just click on desktop menu



- Once you click on desktop it displays the below window, here you can select IP Configuration.

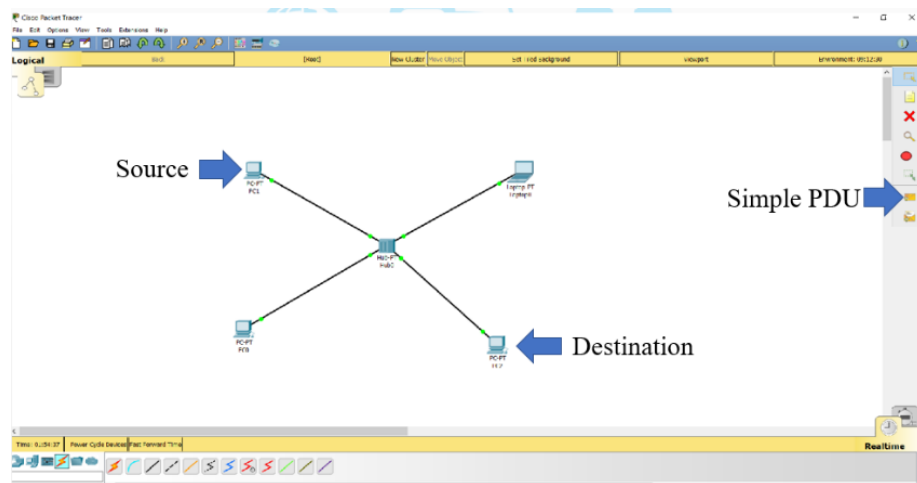


- Click on “static” radio button and give IP address as 10.1.1.1
- Click on Subnet Mask field, it automatically takes subnet mask as 255.255.0.0
- Repeat same procedure for all the end devices to configure IP address.



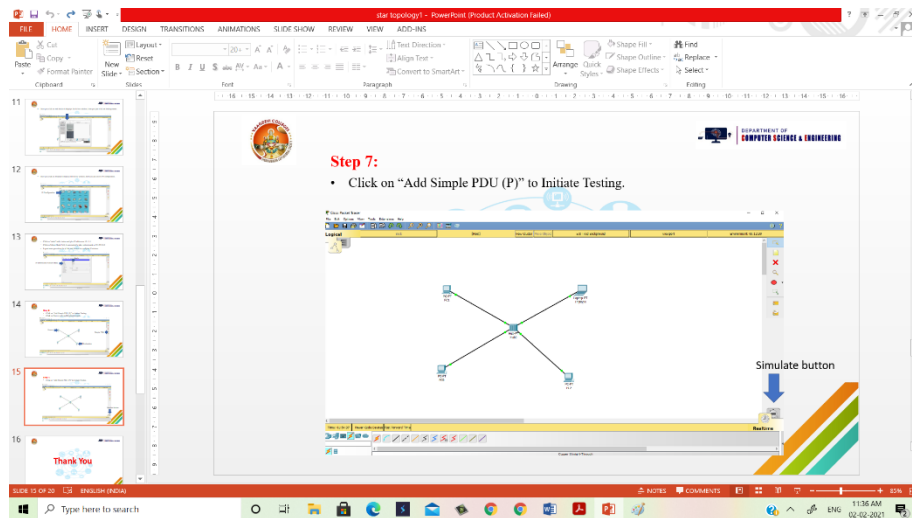
Step 6:

- Click on “Add Simple PDU (P)” to Initiate Testing.
- Click on Source node and Destination node.



Step 7:

- Click on “Add Simple PDU (P)” to Initiate Testing.



EXPERIMENT-7

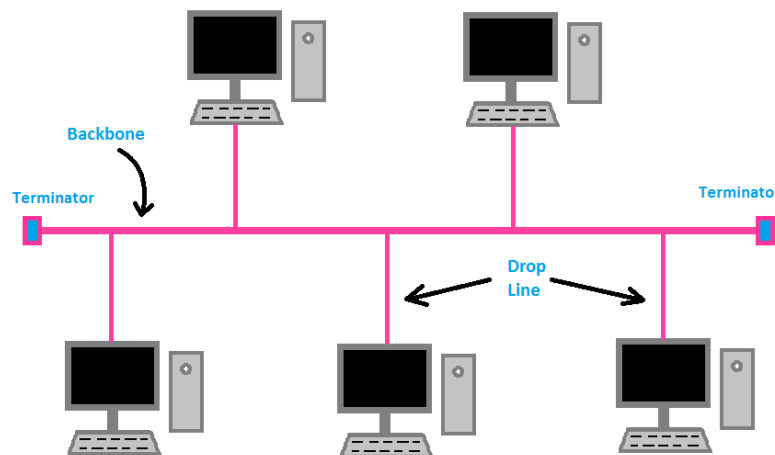
Aim: Configure Bus topology using packet tracer software.

Apparatus (Software): Packet tracer Software

Procedure: To implement this practical following network topology is required to be configured using following steps.

Bus Topology:

Bus topology alternatively referred to as a Line topology. This topology is famously used for the Local Area Network. In this configuration, each computer and network device is connected to a single cable or backbone. Depending on the type of network card used in each computer of the star topology, a coaxial cable or an RJ-45 network cable is used to connect computers together.



Bus Topology

Advantages of Bus topology

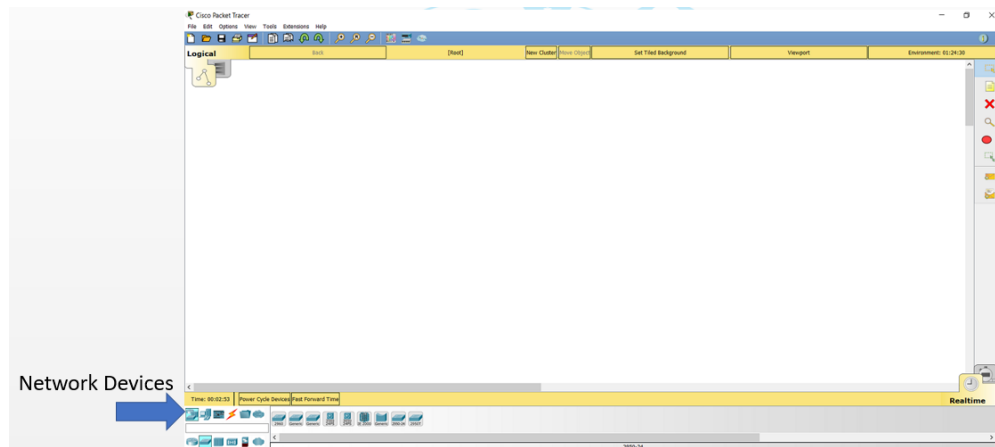
- It works well when you have a small network.
- It requires less cable length than a star topology.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.

Disadvantages of Bus topology

- If the main cable is damaged, the network fails or splits into two.
- Additional devices slow the network down.
- It can be difficult to identify the problems if the whole network goes down.

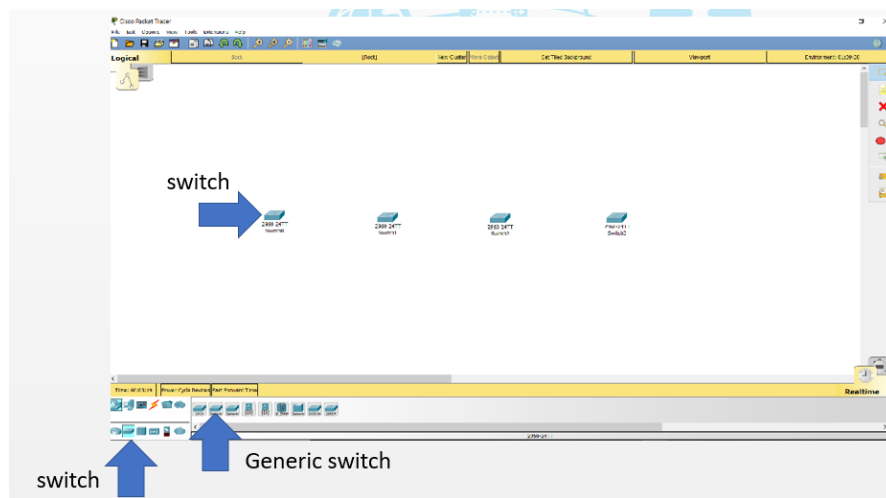
Step 1:

- Open Cisco Packet Tracer and Open Networking Device Menu.



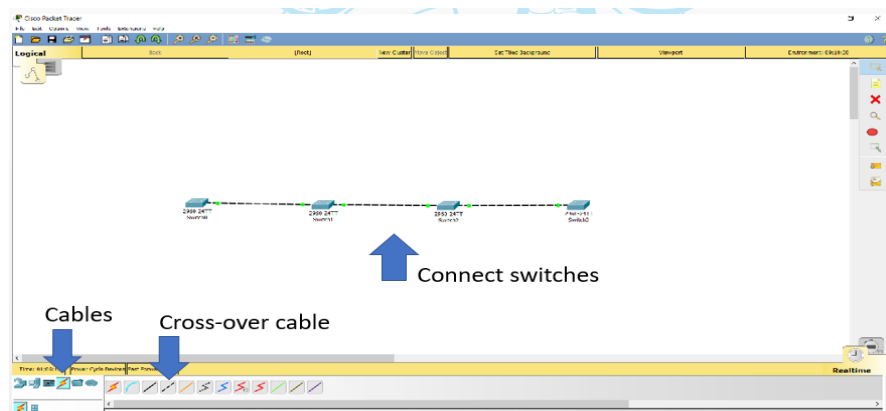
Step 2:

- Click on Switch and select Generic switch.
- Drag selected switch to the work area.



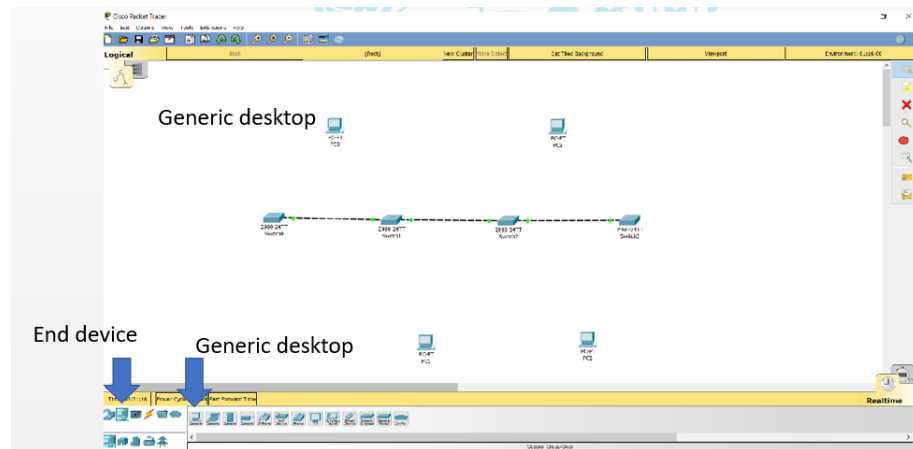
Step 3:

- Click on Cables and select cross-over cable.
- Connect the switches using cross-over cable.



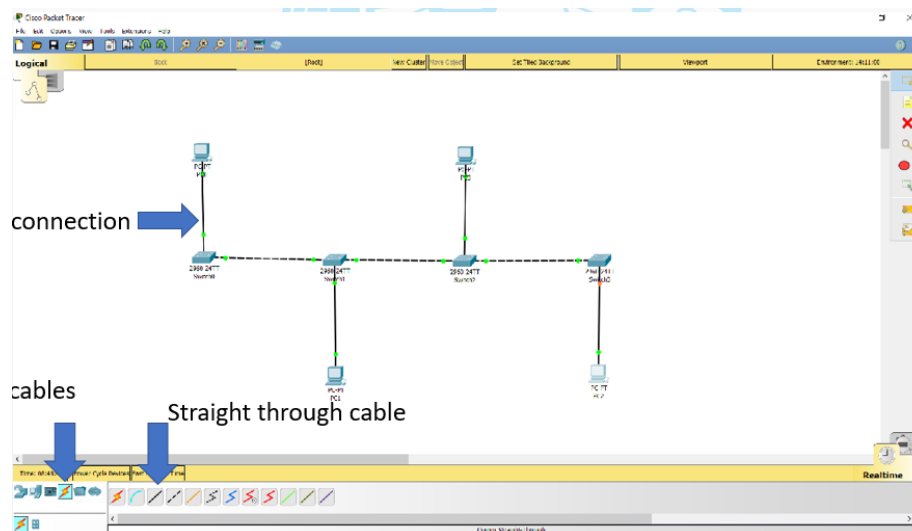
Step 4:

- Click on end devices and select Generic desktop.
- Drag selected end device to the work area.

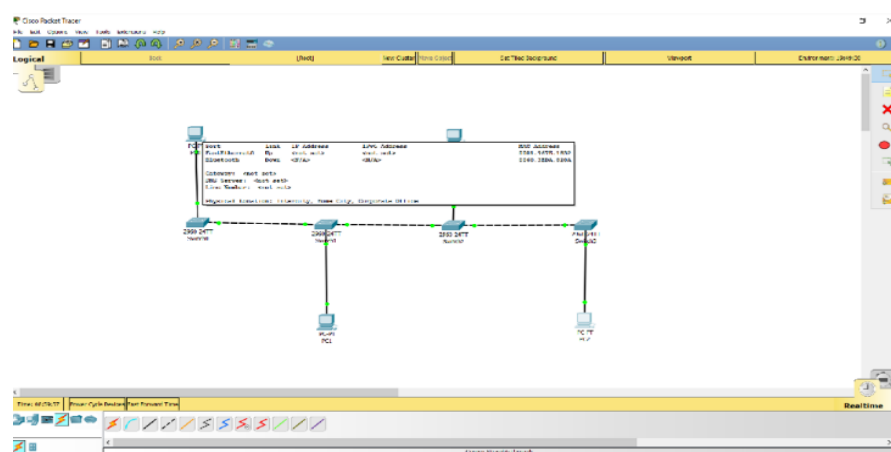


Step 5:

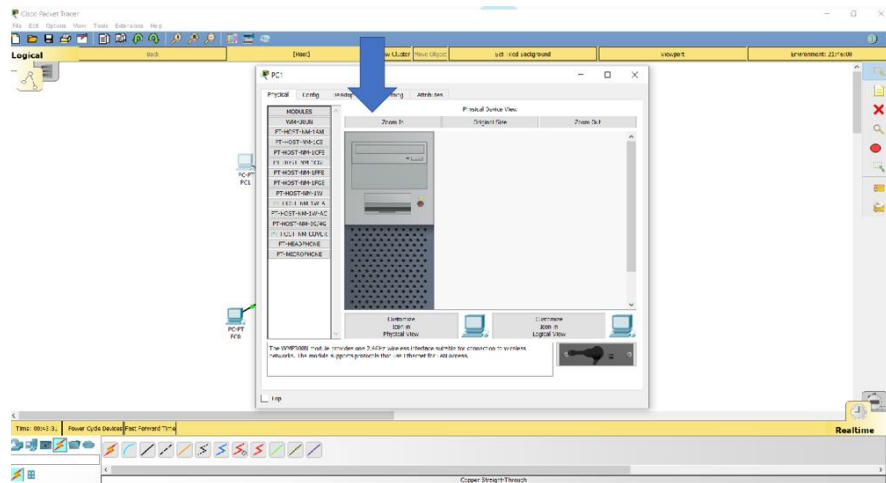
- Choose Connecting Cable for Device Connections
- Click on cables and select straight through cable
- Connect end devices to backbone network.



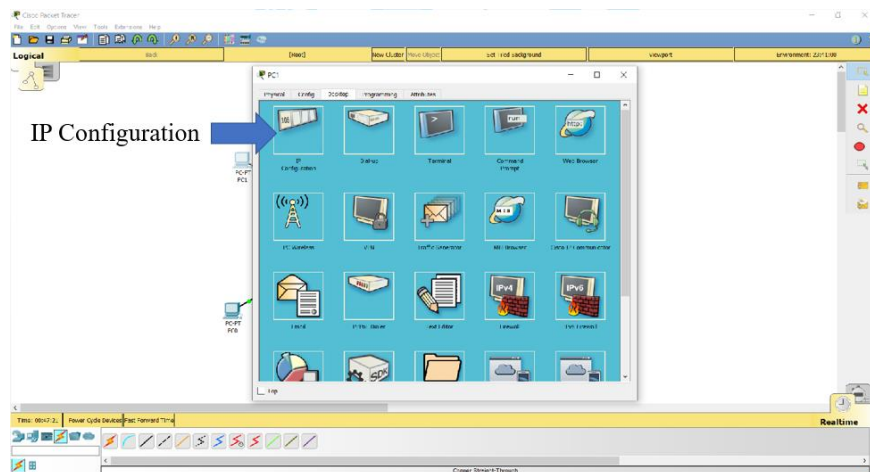
Step 6: Configure IP Address and Subnet Mask



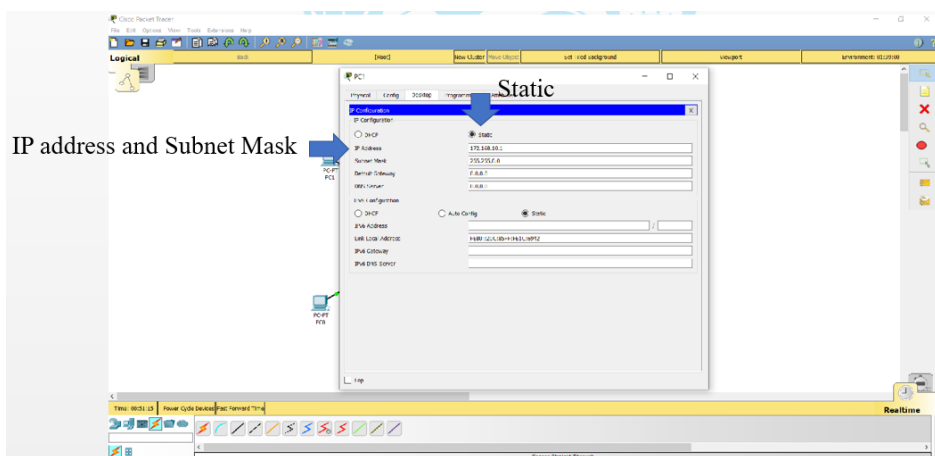
- Once you click on end device it displays the below window, here you just click on desktop menu



- Once you click on desktop it displays the below window, here you can select IP Configuration.

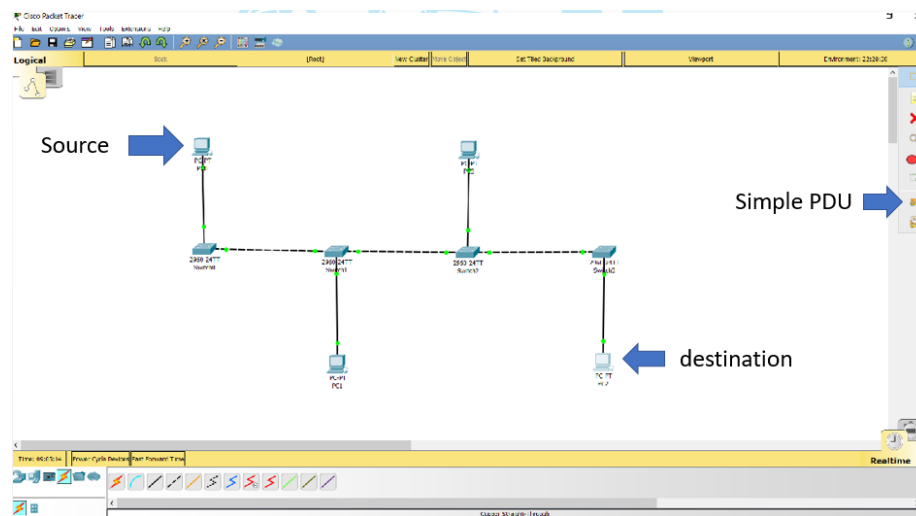


- Click on "static" radio button and give IP address as 10.1.1.1
- Click on Subnet Mask field, it automatically takes subnet mask as 255.255.0.0
- Repeat same procedure for all the end devices to configure IP address.



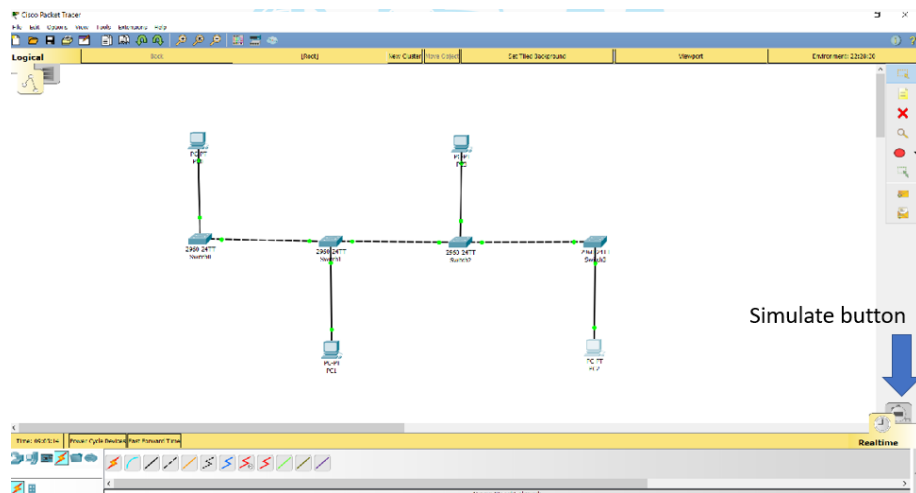
Step 7:

- Click on “Add Simple PDU (P)” to Initiate Testing.
- Click on Source node and Destination node.



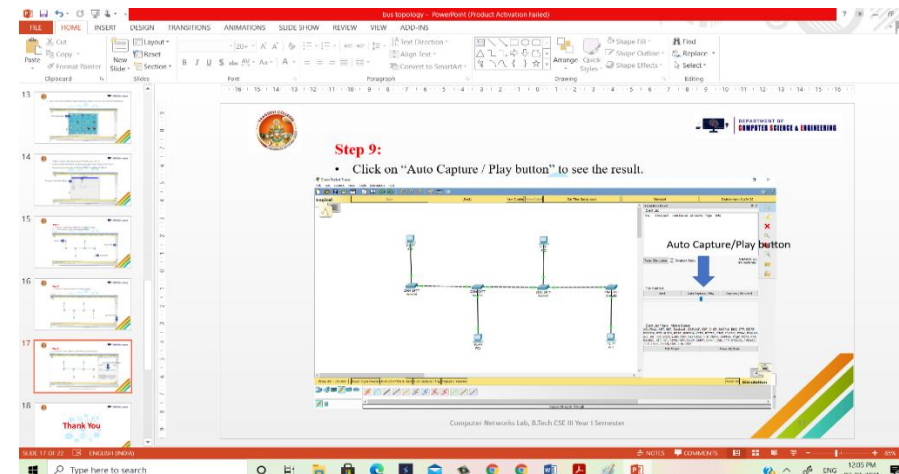
Step 8:

- Click on “Simulate button” to Initiate Testing.



Step 9:

Click on “Auto Capture / Play button” to see the result.



EXPERIMENT-8

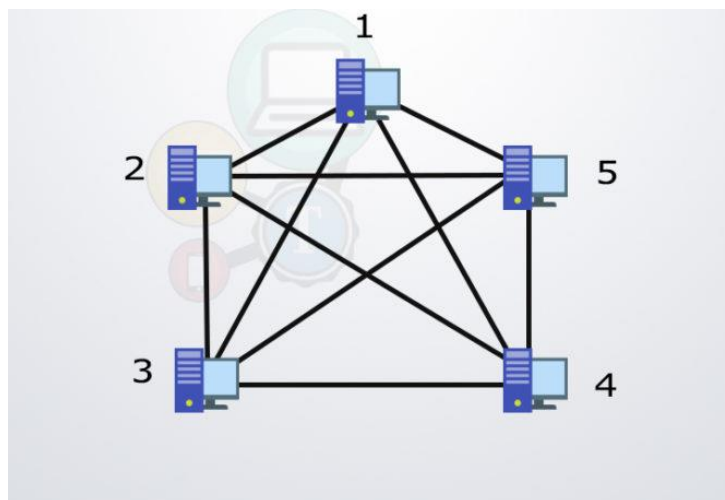
Aim: Configure Mesh topology using packet tracer software.

Apparatus (Software): Packet tracer Software

Procedure: To implement this practical following network topology is required to be configured using following steps.

Mesh Topology:

Mesh topology is one of the most common network setups. In a mesh topology, all the nodes or devices are directly connected to each other. Each Node or Computer contains a dedicated link to every other Node or Computer in the whole Network. Mesh topology can be wired or wireless



Advantages of Mesh topology

- connection can carry its own data load
- It is Robust
- A fault is diagnosed easily
- Provides security and privacy

Disadvantages of Mesh topology

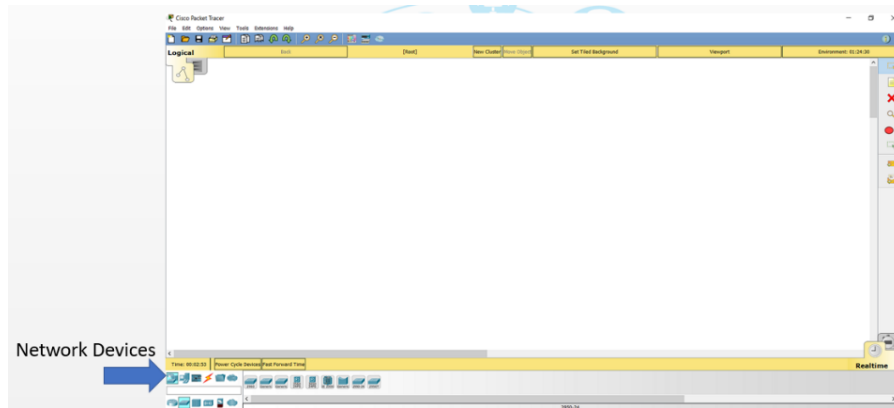
- Installation and configuration are difficult if the connectivity gets more
- Bulk wiring is required
- Cabling cost is more

Practical Examples of Mesh topology

- connection of telephone regional offices in which each regional office needs to be connected to every other regional office.
- Smart Home Control and Monitoring (Zigbee).
- Google Home
- Google Wi-Fi
- Networks in military devices

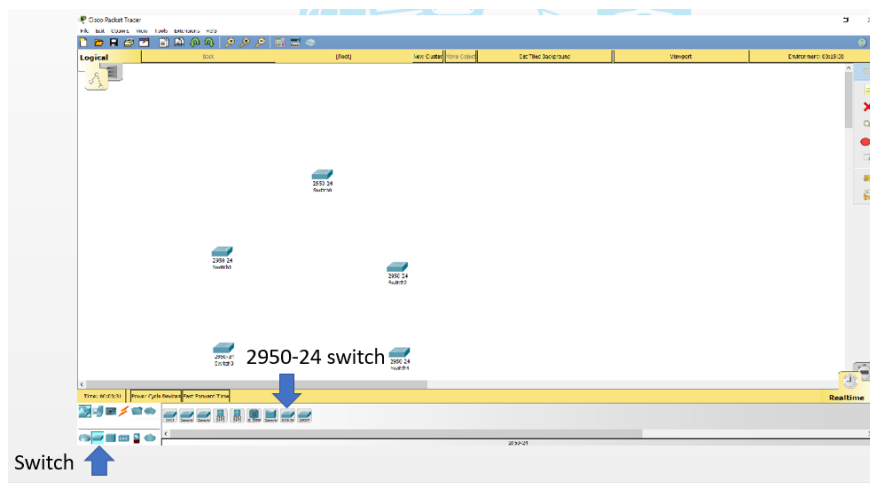
Step 1:

- Open Cisco Packet Tracer and Open Networking Device Menu.



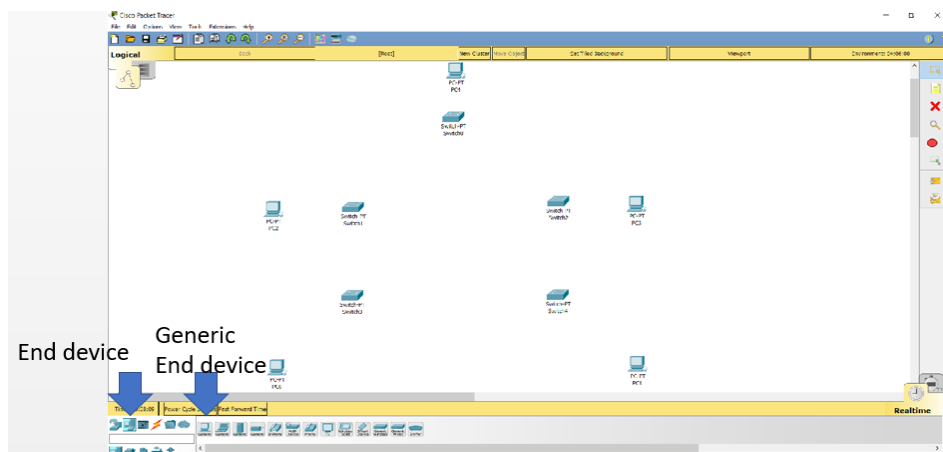
Step 2:

- Select Switch and choose 2950-24 switch
- Drag it onto the work area.



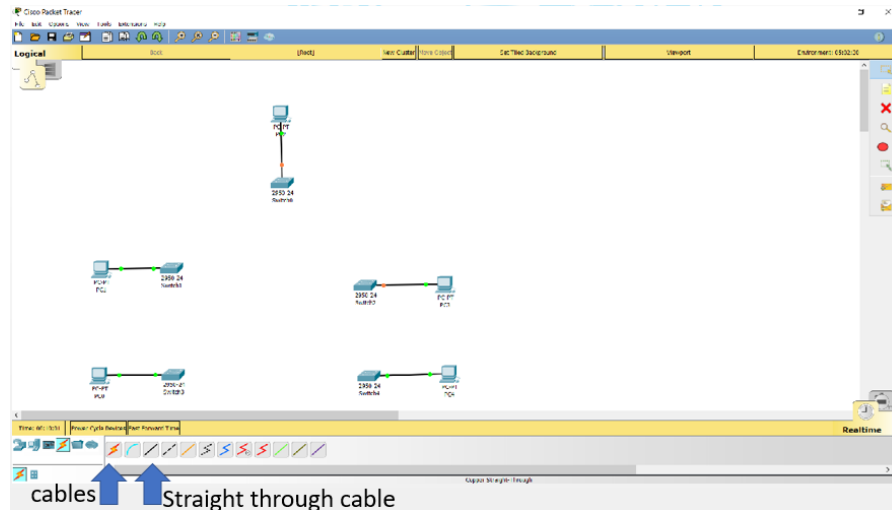
Step 3:

- Click on End Devices and select an end device.
- Drag selected end device to the work area.

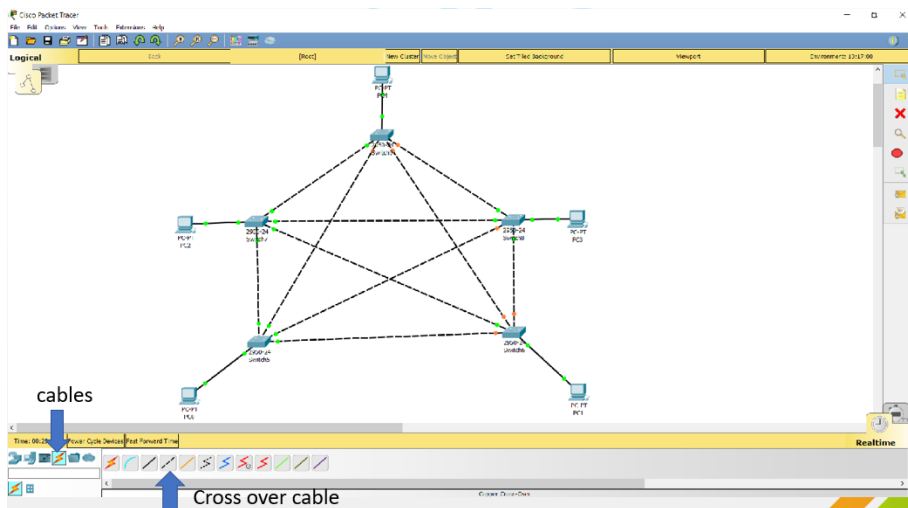


Step 4:

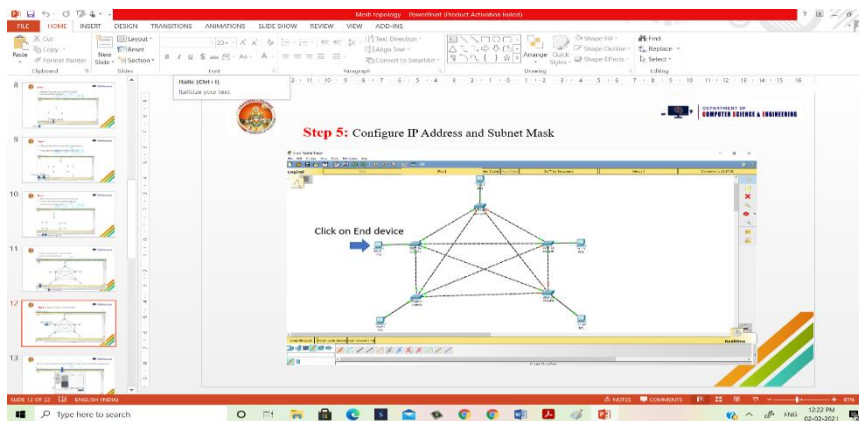
- Choose Connecting Cable for Device Connections
- Click on cables and select straight through cable
- Connect end devices to Switch.



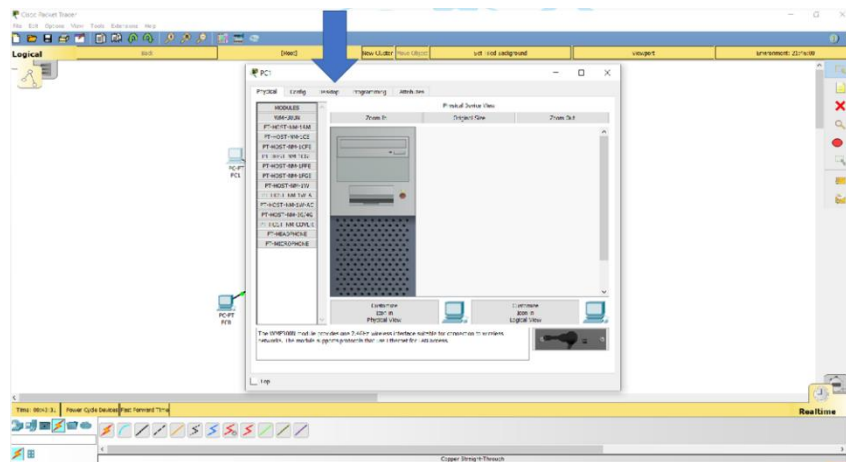
- Click on cables and select cross over cable
- Connect all Network devices.



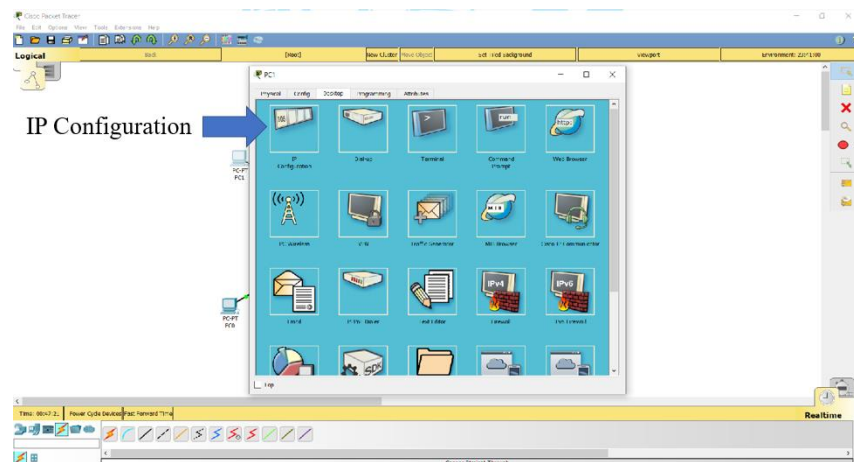
Step 5: Configure IP Address and Subnet Mask



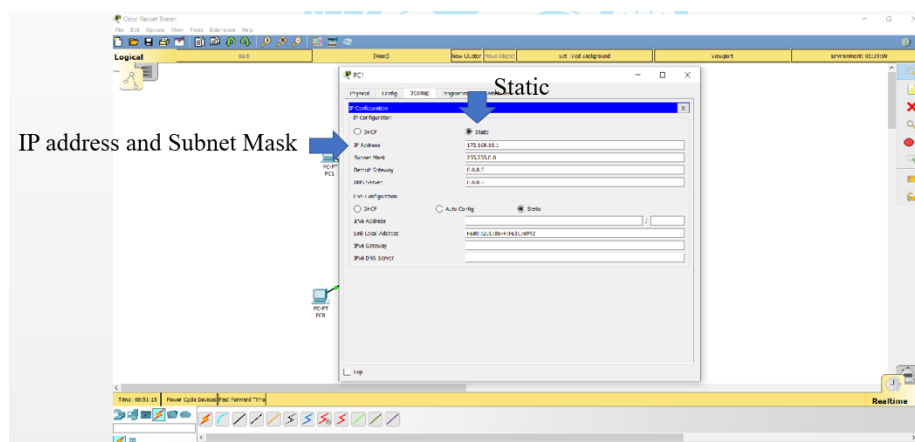
- Once you click on end device it displays the below window, here you just click on desktop menu



- Once you click on desktop it displays the below window, here you can select IP Configuration.

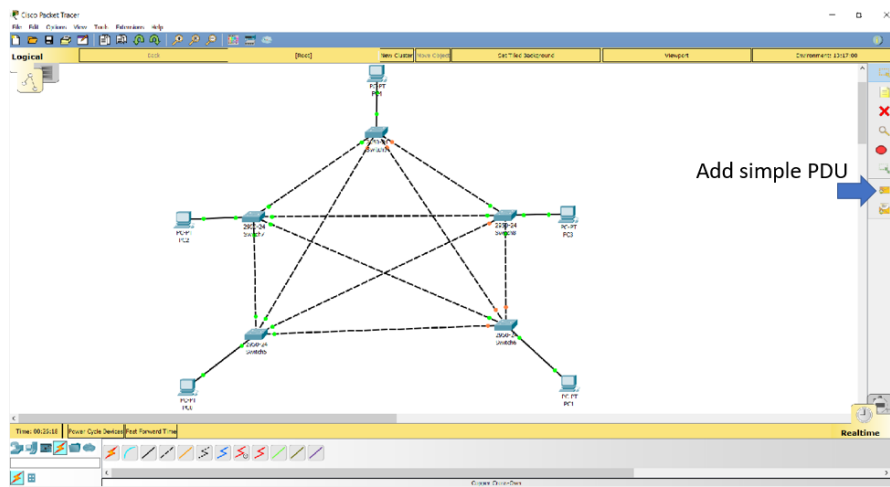


- Click on "static" radio button and give IP address as 10.1.1.1
- Click on Subnet Mask field, it automatically takes subnet mask as 255.255.0.0
- Repeat same procedure for all the end devices to configure IP address.



Step 6:

- Click on “Add Simple PDU (P)” to Initiate Testing.
- Click on Source node and Destination node.



Step 7:

- Click on “Add Simple PDU (P)” to Initiate Testing.

