Practical -3

AIM: To study the Packet tracer tool Installation and User Interface Overview

c) To understand environment of CISCO PACKET TRACER to design simple network.

INTRODUCTION:

A simulator, as the name suggests, simulates network devices and its environment. Packet Tracer is an exciting network design, simulation and modelling tool.

1. It allows you to model complex systems without the need for dedicated equipment.
2. It helps you to practice your network configuration and troubleshooting skills via computer or an Android or iOS based mobile device.
3. It is available for both the Linux and Windows desktop environments.
4. Protocols in Packet Tracer are coded to work and behave in the same way as they would on real hardware.

INSTALLING PACKET TRACER:

To download Packet Tracer, go to **https://www.netacad.com** and log in with your Cisco Networking Academy credentials; then, click on the Packet Tracer graphic and download the package appropriate for your operating system. (Can be used to download in your laptop).

Windows

Installation in Windows is pretty simple and straightforward; the setup comes in a single file named Packettracer_Setup6.0.1.exe. Open this file to begin the setup wizard, accept the license agreement, choose a location, and start the installation.

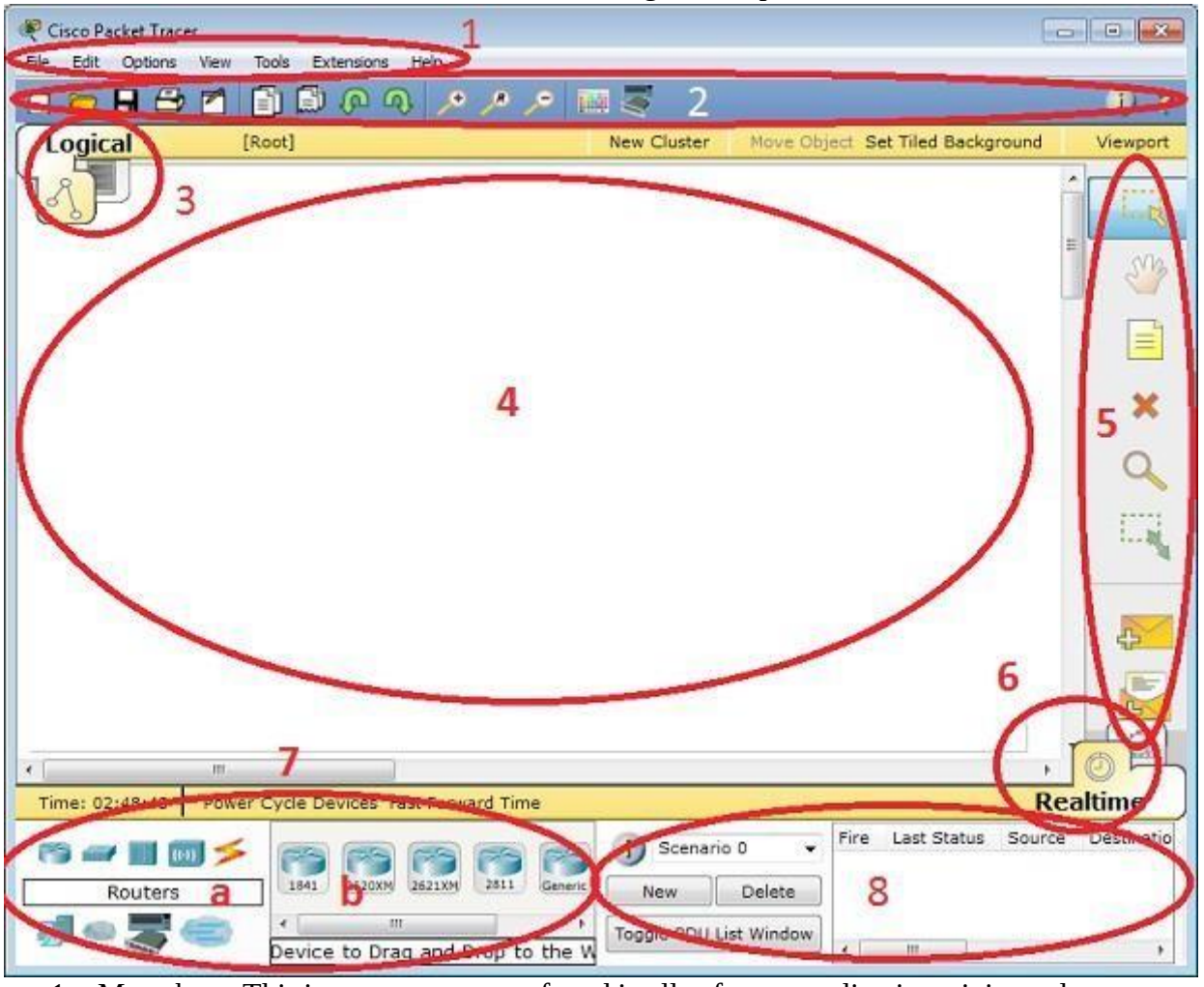
Linux

Linux users with an Ubuntu/Debian distribution should download the file for Ubuntu, and those using Fedora/Redhat/CentOS must download the file for Fedora. Grant executable permission to this file by using chmod, and execute it to begin the installation.

```
chmod +x PacketTracer601_i386_installer-rpm.bin
        ./PacketTracer601_i386_installer-rpm.bin
```

USER INTERFACE OVERVIEW:

The layout of Packet Tracer is divided into several components. The components of the Packet Tracer interface are as follows: match the numbering with explanations.



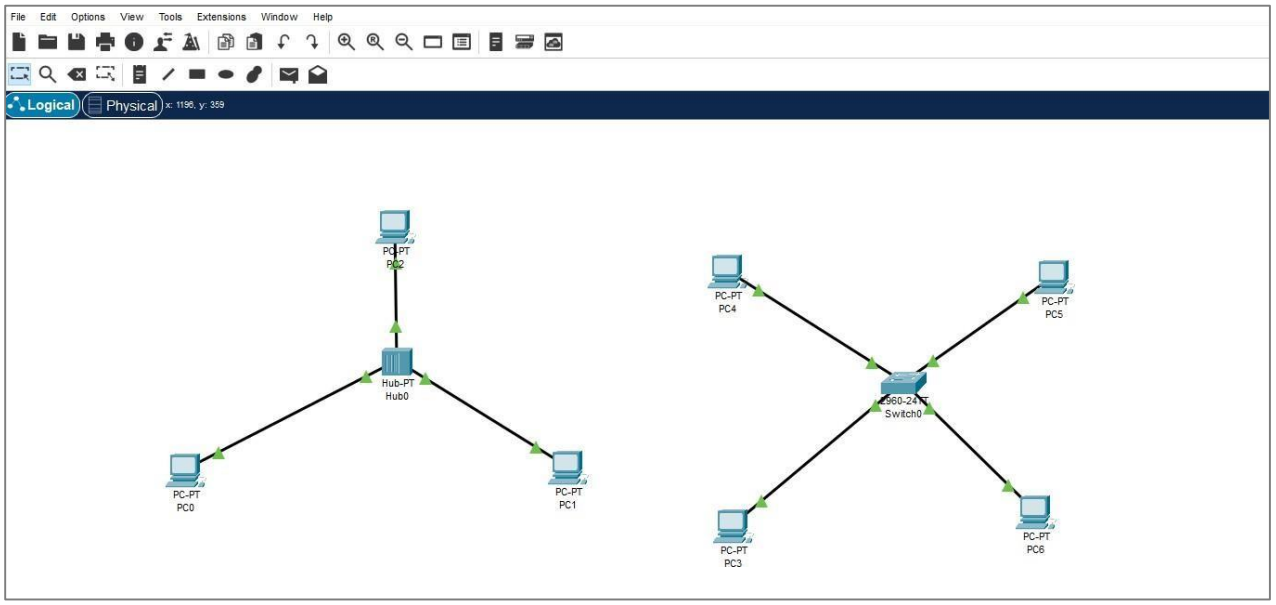
1. Menu bar – This is a common menu found in all software applications; it is used to open, save, print, change preferences, and so on.
2. Main toolbar – This bar provides shortcut icons to menu options that are commonly accessed, such as open, save, zoom, undo, and redo, and on the right-hand side is an icon for entering network information for the current network.
3. Logical/Physical workspace tabs – These tabs allow you to toggle between the Logical and Physical work areas.
4. Workspace – This is the area where topologies are created and simulations are displayed.
5. Common tools bar – This toolbar provides controls for manipulating topologies, such as select, move layout, place note, delete, inspect, resize shape, and add simple/complex PDU.
6. Real-time/Simulation tabs – These tabs are used to toggle between the real and simulation modes. Buttons are also provided to control the time, and to capture the packets.
7. Network component box – This component contains all of the network and end devices available with Packet Tracer, and is further divided into two areas: Area 7a: Device-type selection box – This area contains device categories Area 7b: Device-specific selection box – When a device category is selected, this selection box displays the different device models within that category

8. User-created packet box – Users can create highly-customized packets to test their topology from this area, and the results are displayed as a list.

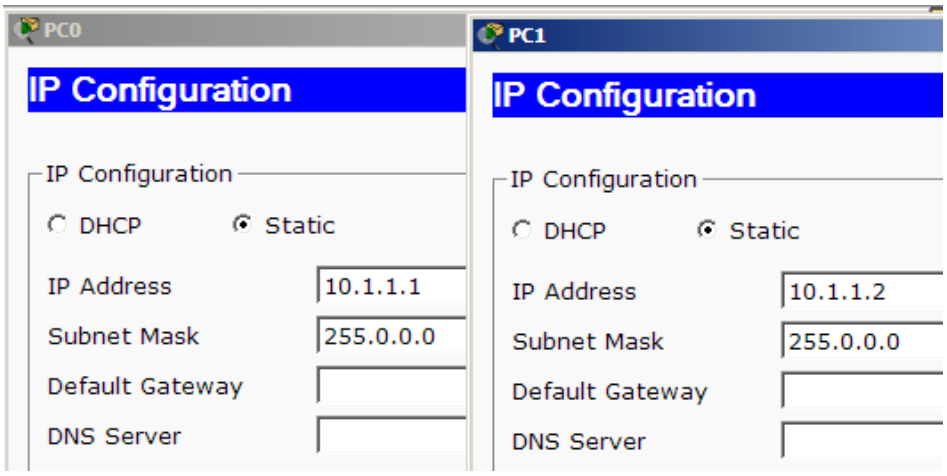
d) Analyse the behaviour of network devices using CISCO PACKET TRACER simulator.

1. From the network component box, click and drag-and-drop the below components:
    a. 4 Generic PCs and One HUB
    b. 4 Generic PCs and One switch

2. Click on Connections:
    a. Click on Copper Straight-Through cable,
    b. Select one of the PC and connect it to HUB using the cable. The link LED should glow in green, indicating that the link is up. Similarly connect remaining 3 PCs to the HUB.
    c. Similarly connect 4 PCs to the switch using copper straight-through cable.



3. Click on the PCs connected to hub, go to the Desktop tab, click on IP Configuration, and enter an IP address and subnet mask. Here, the default gateway and DNS server information is not needed as there are only two end devices in the network.



Click on the PDU (message icon) from the common tool bar,

a. Drag and drop it on one of PC (source machine) and then drop it on another PC (destination machine) connected to the HUB.

4. Observe the flow of PDU from source PC to destination PC by selecting the Realtime mode of simulation.

5. Repeat step #3 to step #5 for the PCs connected to the switch.

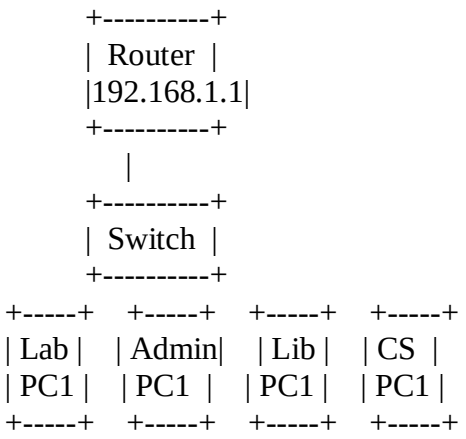
6. Observe how HUB and switch are forwarding the PDU and write your observation and conclusion about the behaviors of Switch and HUB.

Student observation:

a. From your observation write down the behavior of Switch and HUB in terms of forwarding the packets received by them.

b. Find out the network topology implemented in your college and draw and label that topology in your observation book.

From the observations, a network switch operates by intelligently forwarding packets only to the specific port that leads to the destination device. When a switch receives a data packet, it reads the destination MAC address and consults its MAC address table to identify which port is associated with that address. The packet is then sent only through that port, minimizing unnecessary traffic and improving overall network efficiency and security. Switches reduce collisions by creating separate collision domains for each connected device.
In contrast, a network hub works as a simple repeater that broadcasts all packets it receives to every port except the one it came from. It does not analyze the packet content or destination address. Every device connected to the hub receives every packet, regardless of the intended recipient, which increases network traffic and the likelihood of collisions. This behavior makes hubs less efficient and more prone to collisions compared to switches, especially as the number of connected devices grows.


Router
192.168.1.1
Switch
Lab PC1
Admin PC1
Lib PC1
CS PC1