# SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
# FACULTY OF ENGINEERING AND TECHNOLOGY
# SCHOOL OF COMPUTING


## 21CSC302J COMPUTER NETWOKS LAB MANUAL

| Course Code | 21CSC302J | Course Name | COMPUTER NETWORKS | Course Category | C | PROFESSIONAL CORE | L | T | P | C |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | 3 | 0 | 2 | 4 |

| Pre-requisite Courses | Nil | Co-requisite Courses | Nil | Progressive Courses | Nil |
|---|---|---|---|---|---|
| Course Offering Department | School of Computing | Data Book / Codes / Standards | Nil | | |

| Course Learning Rationale (CLR): | The purpose of learning this course is to: |
|---|---|
| CLR-1: | define the layered network architecture |
| CLR-2: | produce knowledge in IP addressing |
| CLR-3: | identify suitable routing algorithms based on geographical location of the devices |
| CLR-4: | apply the concept of Error detection to identify the errors in data |
| CLR-5: | exploring reliable and unreliable protocols |

| Course Outcomes (CO): | At the end of this course, learners will be able to: | Program Outcomes (PO) | | | | | | | | | | | | Program Specific Outcomes | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | | | |
| | | Engineering Knowledge | Problem Analysis | Design/development of solutions | Conduct investigations of complex problems | Modern Tool Usage | The engineer and society | Environment & Sustainability | Ethics | Individual & Team Work | Communication | Project Mgt. & Finance | Life Long Learning | PSO-1 | PSO-2 | PSO-3 |
| CO-1: | apply the knowledge of communication | 3 | - | - | - | 3 | - | - | - | - | - | - | - | 1 | - | - |
| CO-2: | construct the network using addressing schemes | 3 | - | - | 2 | - | - | - | - | - | - | - | - | 1 | - | - |
| CO-3: | design and implement the various Routing Protocols | 3 | - | - | 2 | 3 | - | - | - | - | - | - | - | 1 | - | - |
| CO-4: | identify and correct the errors in transmission | 3 | - | - | - | - | - | - | - | - | - | - | - | 1 | - | - |
| CO-5: | analyze the services provided by Transport and Application layers | 3 | - | - | - | - | - | - | - | - | - | - | - | 1 | - | - |

| Session 2 Periods | Exercise | CLO | Page No |
|---|---|---|---|
| Lab 1 | 1.a - Introduction to Packet Tracer | | |
| | 1.b - Networking Commands (Windows/ Unix) | | |
| | 1.c – Study of Cables and it's color codes | | |
| Lab 2 | Implementation of Network Topologies | | |
| | 2. a - Demonstration of cross over cable with P-P network | | |
| | 2 .b - Demonstration of straight-through cable with local area network | | |
| Lab 3 | Configuration of IP Address in Router | | |
| Lab 4 | Subnetting in WAN Configuration (DTE and DCE) | | |
| Lab 5 | 5. a - VLAN Switch Configuration | | |
| | 5. b - Router Configuration through a Console cable | | |
| Lab 6 | 6. a Demonstration of Static Routing | | |
| | 6. b Demonstration of Default Routing | | |
| Lab 7 | 7. a Demonstration of RIP v1 | | |
| | 7. b Demonstration of RIP v2 | | |
| Lab 8 | EIGRP Configuration, Bandwidth, and Adjacencies | | |
| Lab 9 | EIGRP Authentication and Timers | | |
| Lab 10 | Single-Area OSPF Link Costs and Interface | | |
| Lab 11 | Multi-Area OSPF with Stub Areas and Authentication | | |
| Lab 12 | Examining Network Address Translation (NAT) | | |
| Lab 13 | BGP Configuration | | |
| Case Study Implementation | | | |

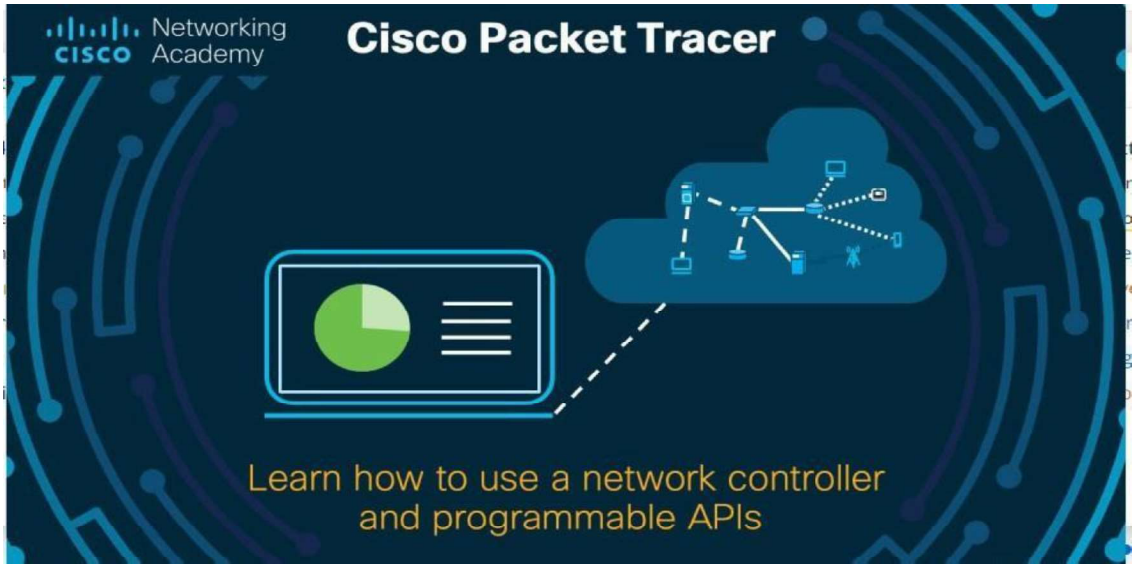
## EXERCISE 1

**AIM:**

To understand the basics of Packet Tracer, Networking commands and Study of different types of cables

### 1.1 INTRODUCTION TO PACKET TRACER

Cisco Packet Tracer is a free application that enables you to practice network configuration and troubleshooting on your desktop or laptop computer. It enables you to mimic networks without having physical access to the underlying hardware. Along with networking, you may improve your Internet of Things (IoT) and cybersecurity skills through education and practice. You have the option of creating a network from scratch, using a pre-built sample network, or completing lab projects. While Packet Tracer is not a substitute for practising on physical routers, switches, firewalls, and servers, it does offer a number of advantages.

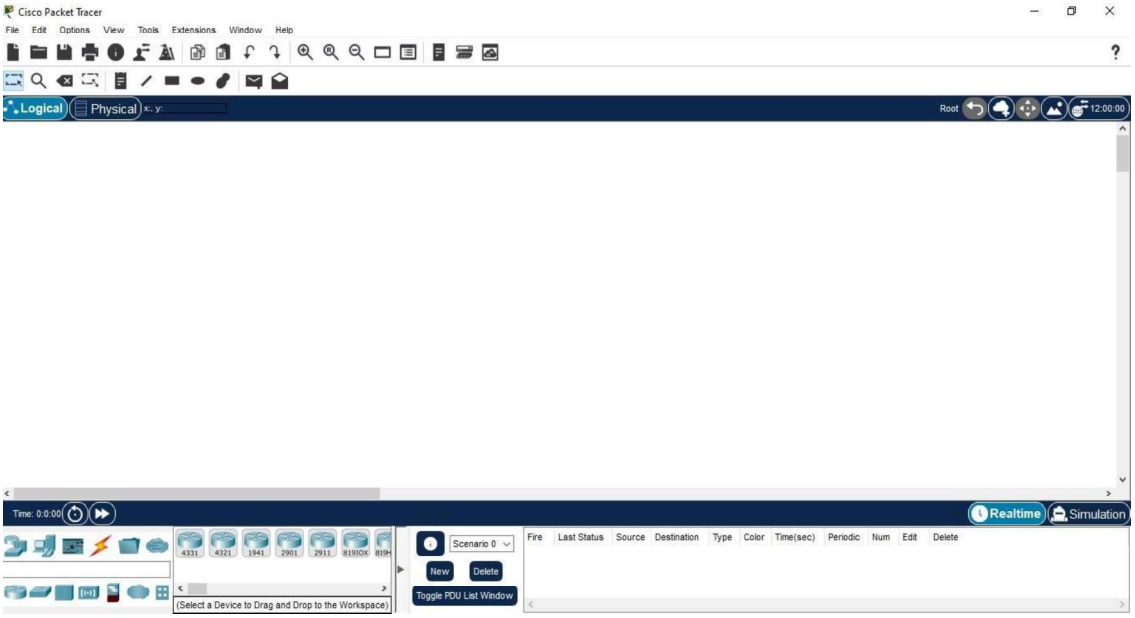



### 1.a What are the Benefits of Using Packet Tracer?

Imagine being able to peer inside a small business network or the internet. Have you ever wished to create an Internet of Things system that would notify you through the phone if there was an issue in your home environment? Welcome to Cisco Packet Tracer, the simulation environment that may assist you in doing all of these tasks and more. It is intended to familiarize you with the Cisco Packet Tracer network simulation and visualization tool.

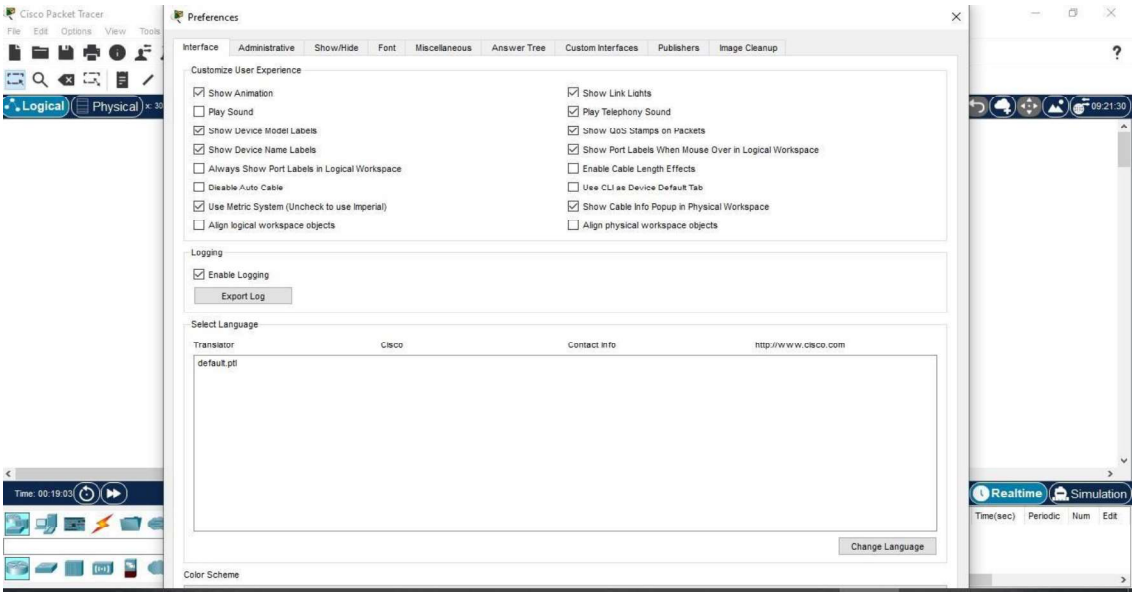
In Packet Tracer, you will design your own network (PT). Additionally, you will learn about the many sorts of PT files.

## 1.b Packet Tracer UI:




Packet Tracer is a tool that allows you to simulate real networks. It provides three main menus that you can use for the following:

- Add devices and connect them via cables or wireless.
- Select, delete, inspect, label, and group components within your network.
- Manage your network.



The network management menu lets you do the following:

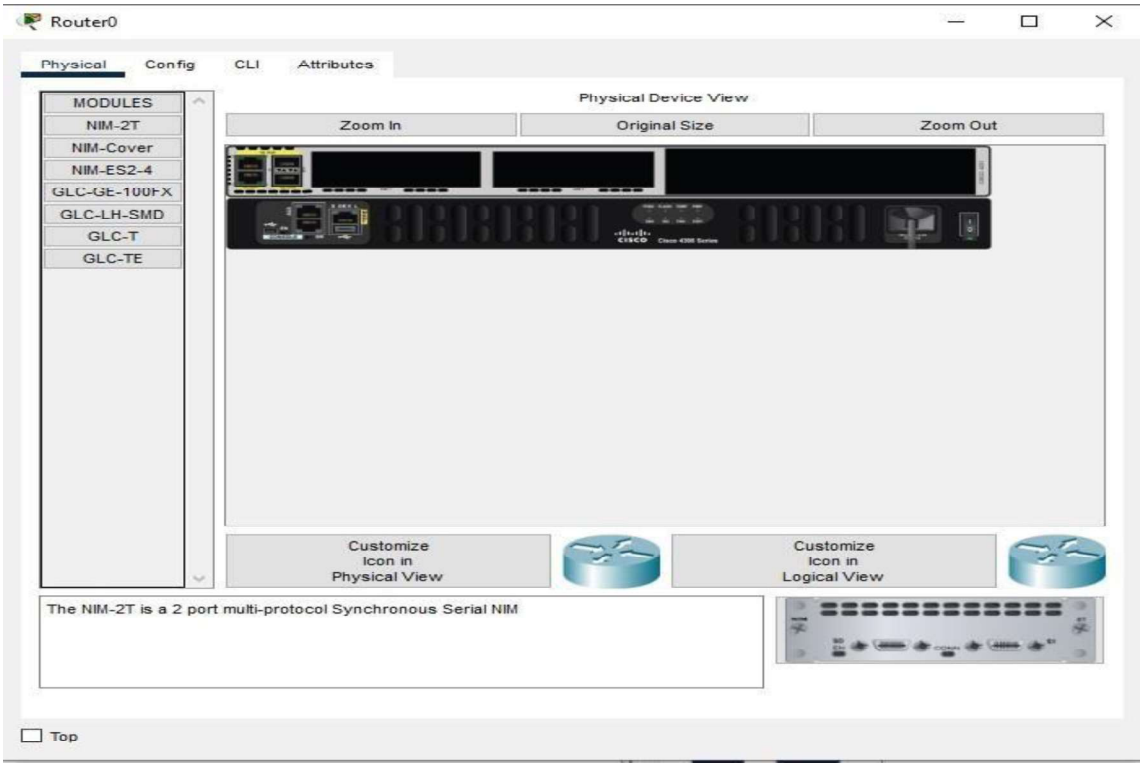
- Open an existing/sample network.
- Save your current network.
- Modify your user profile or your preferences.

Packet Tracer also provides a variety of tabs for device configuration including the following:

- Physical
- Config
- CLI
- Desktop
- Services

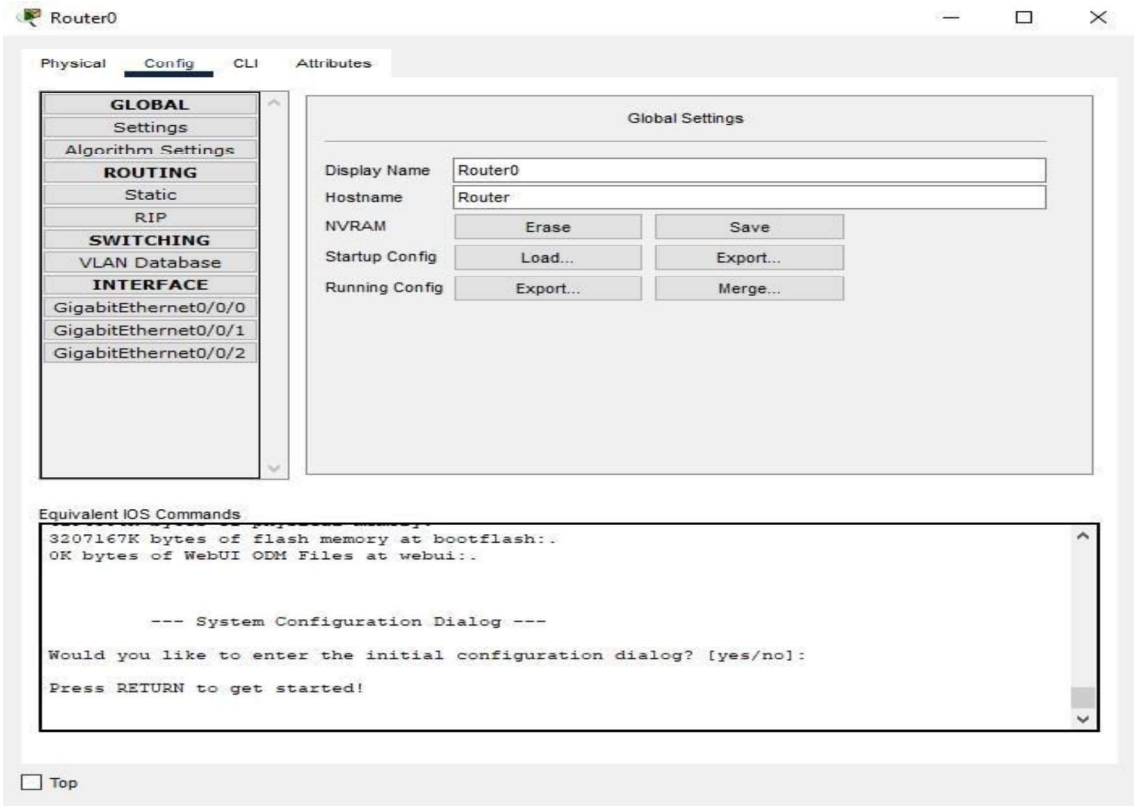
The tabs that are shown depend on the device you are currently configuring.

**Physical Tab**




The Physical tab provides an interface for interacting with the device including powering it on or off or installing different modules, such as a wireless network interface card (NIC).

**Config Tab**

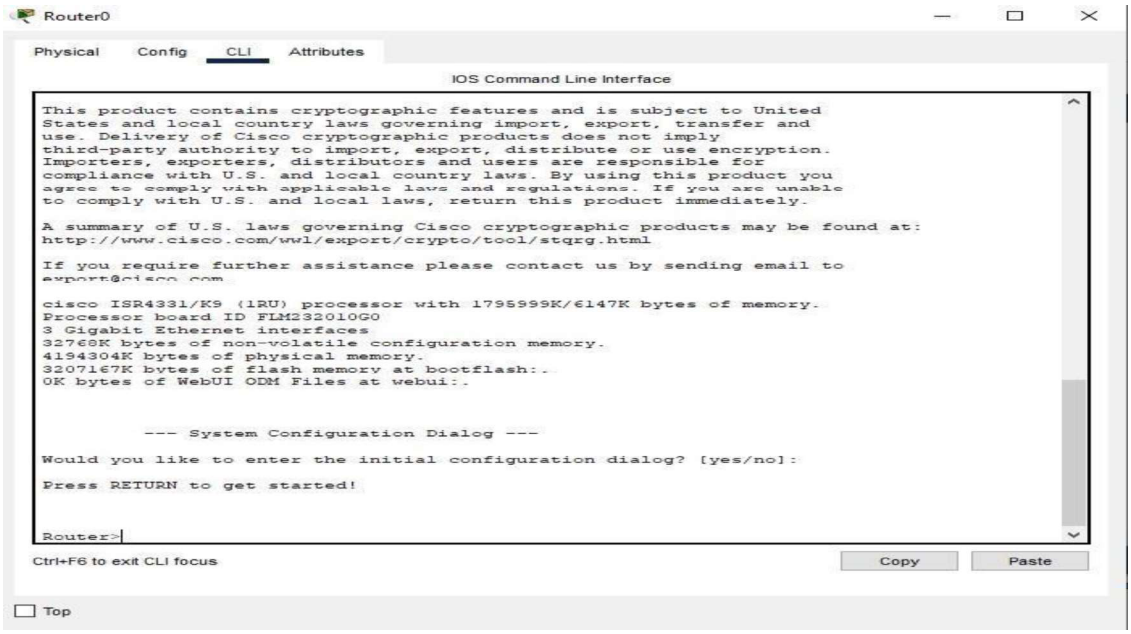



For intermediate devices such as routers and switches, there are two ways to access device configurations. Configurations can be accessed via a Config tab, which is a Graphical User Interface (GUI). Configurations can also be accessed using a command line interface (CLI).

The Config tab does not simulate the functionality of a device. This tab is unique to Packet Tracer. If you don't know how to use the command line interface, this tab provides a way to use a Packet Tracer-only GUI to configure basic settings. As settings are changed in the GUI, the equivalent CLI commands appear in the Equivalent IOS Commands window. This helps you to learn the CLI commands and the Cisco Internetwork Operating System (IOS) while you are using the Config tab.

For example, in the figure, the user has configured MyRouter as the name of the device. The Equivalent IOS Commands window shows the IOS command that achieves the same results in the CLI. In addition, device configuration files can be saved, loaded, erased, and exported here.

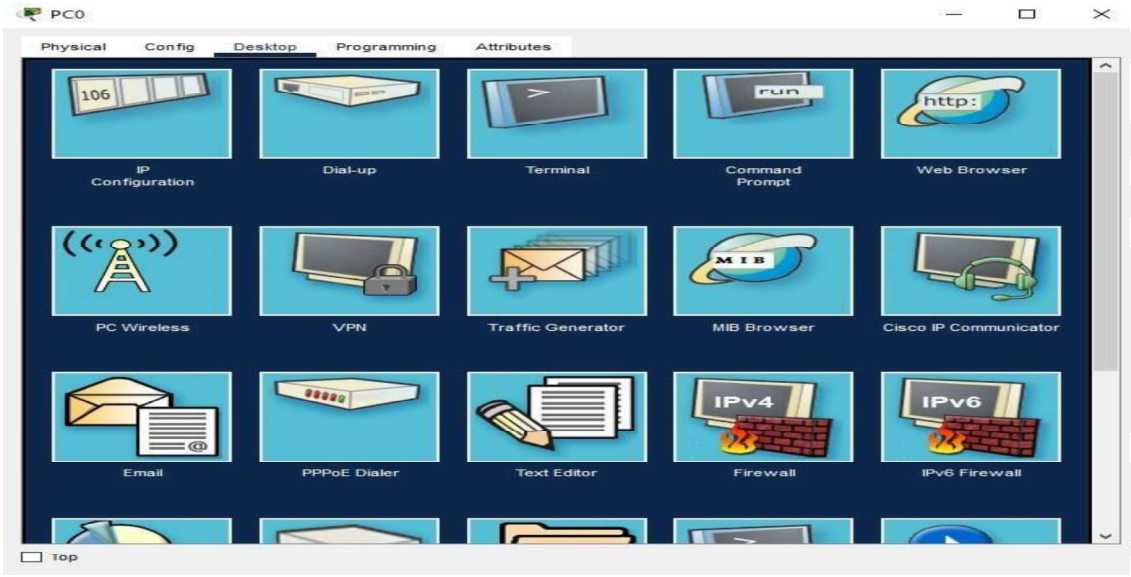
## CLI Tab




The CLI tab provides access to the command line interface of a Cisco device. Using the CLI tab requires knowledge of device configuration with IOS. Here, you can practice configuring Cisco devices at the command line. CLI configuration is a necessary skill for more advanced networking implementations.

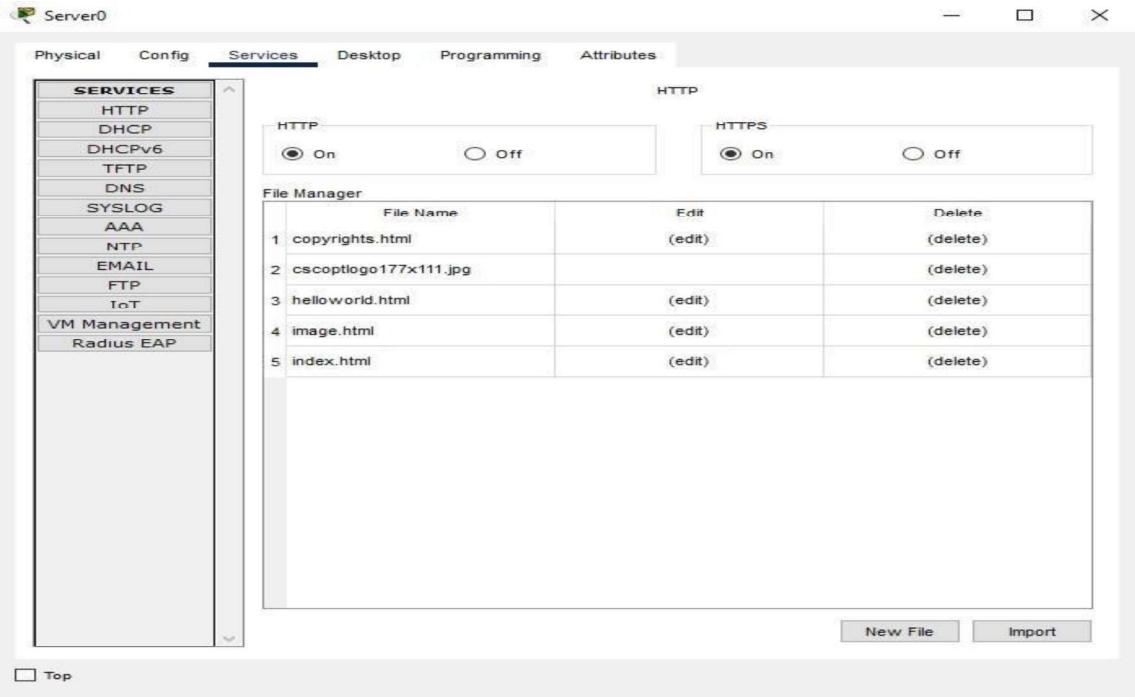
Note: Any commands that were entered from the Config tab are also shown in the CLI tab.

## Desktop Tab




For some end devices, such as PCs and laptops, Packet Tracer provides a desktop interface that gives you access to IP configuration, wireless configuration, a command prompt, a web browser, and other applications.

**Services Tab**




A server has all of the functions of a host with the addition of one more tab, the Services tab. This tab allows a server to be configured with common server processes such as HTTP, DHCP, DNS, or other services, as shown in the figure.

## 1.b) NETWORKING COMMANDS

**Ping (Unix/Windows)**

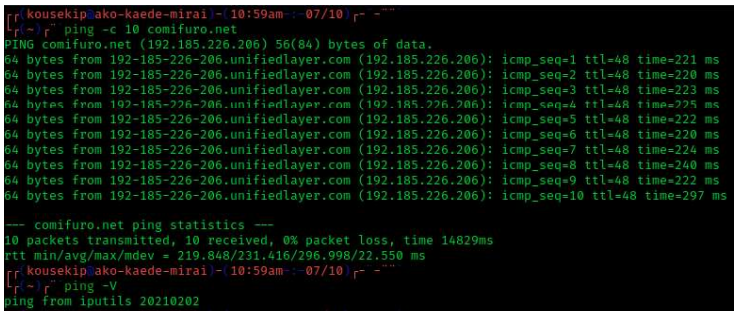
Ping dates from the 70s and is known for being one of the most basic network commands. However, it is not as simple as we believe and has many more uses than those we already know. It is based on the ICMP protocol and is used to determine:

- If there is connectivity between your machine and another machine on the network.
- It's used to measure the "speed" or latency time.

It is a command that exists on all operating systems that support TCP/IP, and it is a basic command that you should know.

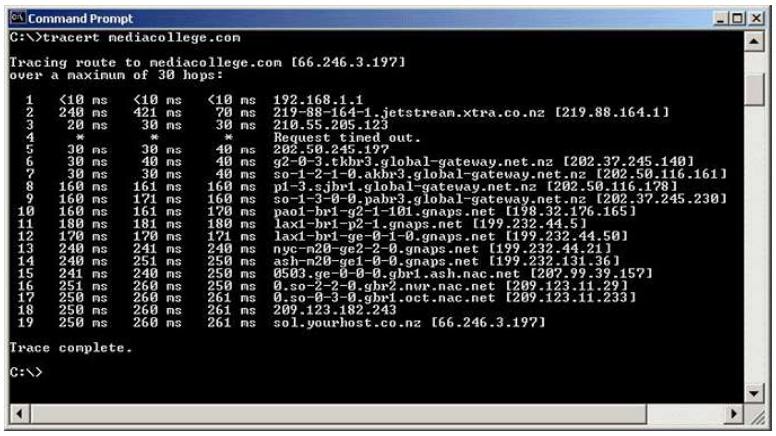
Ping is known for having dozens of parameters and the one that we find more useful is the one responsible for monitoring "the number of packages to send." There are networks that undo the first package, so it is essential to send at least three so we can check that at least one has arrived without being discarded. For this, we use the -c parameter.

The same technique can be used to determine the loss percentage of packages in our network, sending ten packages and seeing if any gets lost. The number of packages that usually get lost in the network will surprise you. (This tool is included in Pandora FMS)
Execution: Ping name/System IP




**Traceroute (Unix/Windows)**

The main objective of this tool is to know the traveling path of a package through our network. This network command will tell us where the package is going through (machines, switches, routers) and check that our network is working properly. If you encounter any problems, it will allow us to have a rough idea about where the fault lies.




Execution:

traceroute –n (on Unix / Linux)

tracert –d (on Windows)

**Arp (Unix/Windows)**

This network command is used to change and view the ARP table, which contains the mappings between the IP address and the MAC address. It only sees the connections in our local area network segment (LAN), so it could be called “low level”. However, it’s used to discover what machines are directly connected to our host or what machines we are connected to. It is a diagnostic tool, and sometimes it can be interesting to monitor it in order to discard ARP Poisoning attacks, which are one of the most common forms of phishing attacks in local networks.

Execution: arp –a

**Curl and wget (Unix/ Windows)**

These are essential commands to do HTTP, HTTPS or FTP requests to remote servers. It allows you to download files or whole web pages, even recursively (it literally allows us to make a “copy” of a website, including images). It supports cookies and allows you to send POST requests, in addition to “simulate a” user agent, use a http proxy or even a SOCKS4/5 proxy.

One of the most common utilities in integration with Pandora FMS, is to verify the contents of a specific web page. Because wget / curl allows us to download the entire contents of a web, it is easy to compare the MD5 of that content with a value previously verified. If it changes, it means that the Web has been altered.

**Netstat (Unix/Windows)**

Network command identifies all TCP connections and UDP open on a machine. Besides this, it allows us to know the following information:

- Routing tables to meet our network interfaces and its outputs.
- Ethernet statistics that show sent and received packages and possible errors.
- To know the id of the process that is being used by the connection.
- Netstat is another basic command as Ping that meets many elementary functions.

**Whois (Unix/ Windows)**

This network command is used to query data domains: to find out who owns the domain, when that domain expires, to view the configured logs, contact details, etc. Its use is highly recommended to contact the administrators of the domains or when incidents of migration of services such as mail and web happen.

To use 'whois' on Windows you need to download the software from this url: https://technet.microsoft.com/en-us/sysinternals/whois.aspx

**VNStat**

It is one of the most complete network commands. It works on all Linux and BSD systems, and allows us to monitor network traffic from the console.

- Installation is simple and fairly quick, allowing monitoring of all network interfaces.
- With VNStat we can collect all traffic needed from any configured interface.
- One of the big differences between VNStat and other tools is that VNStat collects kernel data instead of the interface itself, which means a lighter execution for the system.
- It will not require administrator permissions to run.
- It has the ability to store gathered information so your information never goes missing, even if the system crashes or reboots itself.
- You can set Vnstat to listen to traffic, daily or by billing period, as well as many other options.
- It stands out for its flexibility when configuring the reading of traffic.

Finally, it is possible to set Vnstat output to generate console graphics and even customize them with colours.

**SSH (Unix/Linux/Windows)**

Command to run terminals on remote machines safely. SSH allows any user to run a console just by registering and entering his credentials. So you can run the commands you want as if you were in local.

**More details you need to know about SSH:**

Putty is recommended when using SSH in Windows. You can find it here: http://www.putty.org/

**TCPDump (Unix/Linux/Windows)**

It is one of the "basic" tools of network commands, and when used right, goes on to become a great ally for network administrators, system administrators or programmers.

TCPDump is an advanced command used to inspect traffic from different interfaces of a machine so you can get the exchanged packages. You can dump output to file so then you can analyse it with more powerful sniffers and graphical interfaces such as Wireshark. For Windows, you must use WinDump.

**Ngrep (Unix/Linux/Windows)**

- The grep command power is taken to the network.
- It is a TCPDump with a substring text filter in real time.
- It has a very powerful filtering system for regular expressions and it is typically used to process files generated by tcpdump, wireshark, etc.
- It is a communication package filter over HTTP, SMTP, FTP, DNS and other protocols.

**NMAP (Unix/Windows)**

NMAP is considered the father of the general network scanners. Although today there are more reliable tools for some tasks (like Fping), NMAP is a very versatile tool for scanning networks. It is used to determine which hosts are alive in a network and to do different ways of scanning.

**Netcat (Windows/Unix)**

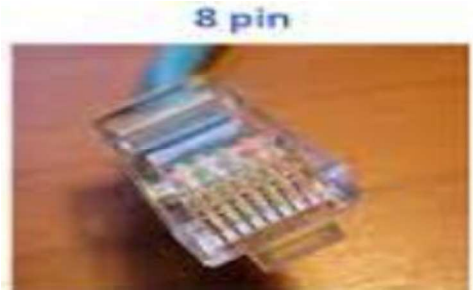
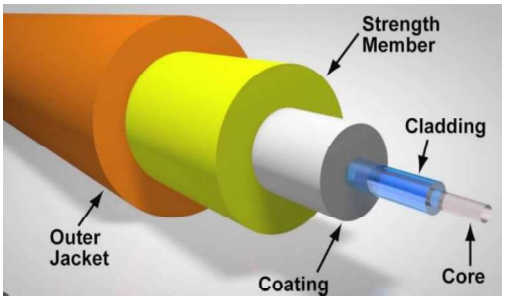
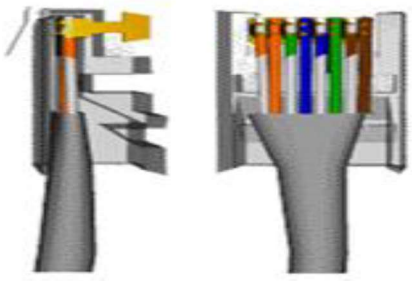
NetCat, or NC, is the network command most versatile that exists nowadays and one of the lightest. However, its use requires some imagination. Only if you've played with scripting, you will understand the subtlety of its name: NetCat. It is a tool designed to be used as a destination of a redirect (one pipe or |). It is used to send or receive information about a connection. For example, a WEB request to service would be something as simple as:

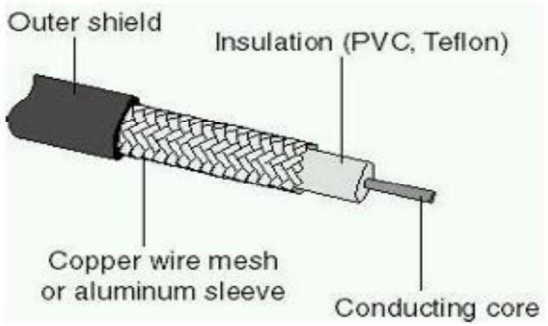
echo -e "GET http://pandorafms.com HTTP/1.0\n\n" | nc pandorafms.com 80

**IPtraf (Linux)**

Special command to obtain traffic statistics. It has a ncurses interface (text) to analyze real-time traffic passing through an interface. It allows you to work at low-level and to see what pairs of connections are established on each machine, and to see in detail the traffic connection of every pair, all in real-time.

## 1.C – Study of Cables & it's Color codes

| Term | Description | Cross Sectional Diagram |
|---|---|---|
| **BNC** | British Naval Connector is the connector used with coaxial cables. |  |
| **RJ – 11** | A registered jack 11 is a telephone connector used on modern telephone lines. |  |
| **RJ – 45** | A registered jack 45 is an eight-wire connector used to connect computers to category 5 unshielded twisted pair (UTP) cables in a network. |  |
| **Fiber Optic Cable** | Fiber optic cable uses light to transmit information across a network. The core of the cable is made of glass, which is protected by a layer of gel or plastic. A plastic cover surrounds the entire cable. |  |
| **UTP** | Unshielded Twisted-Pair Cable is network cable that consists of up to 4 pairs of wires. Each pair is twisted around each other at a different rate and the entire cable is encased in a protective plastic covering. The twisting of the wires in cables is to help prevent EMI (Electro- Magnetic Interference). |  |

| | | |
|---|---|---|
| **Coaxial Cable** | Thin coaxial cable is often referred to as ThinNet. It consists of a copper wire surrounded first by a layer of plastic, then a layer of metal mesh and a final layer of protective plastic. It is used for peer-to-peer networking |  |

**NETWORK DEVICES:**

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:** An **Ethernet hub**, **active hub**, **network hub**, **repeater hub**, **hub** or **concentrator** 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.

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.

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.

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.

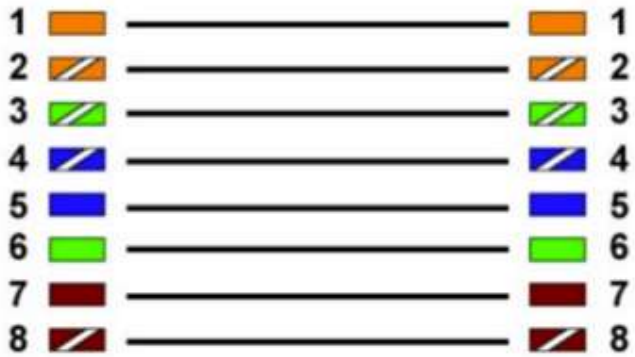
## Exercise 2: Cabling – Straight Through and Cross-over Cabling

**Ethernet cable:**

An Ethernet cable is a network cable used for high-speed wired network connections between two devices. This network cable is made of four-pair cable, which is consists of twisted pair conductors. It is used for data transmission at both ends of the cable, which is called RJ45 connector.

The Ethernet cables are categorized as Cat 5, Cat 5e, Cat 6, and UTP cable. Cat 5 cable can support a 10/100 Mbps Ethernet network while Cat 5e and Cat 6 cable to support Ethernet network running at 10/100/1000 Mbps.

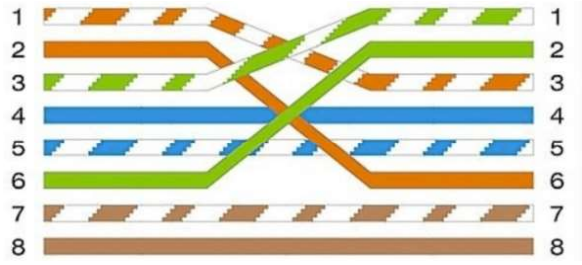
**Straight Through Cable:**




**Straight Through Cable**

Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out. It is in accordance with either the T568A or T568B standards. It uses the same color code throughout the LAN for consistency. This type of twisted-pair cable is used in LAN to connect a computer or a network hub such as a router. It is one of the most common types of network cable.

**Crossover Cable:**




**Crossover Cable**

A Crossover cable is a type of CAT 5 where one end isT568A configuration and the other end as T568BConfiguration. In this type of cable connection, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6.

Crossover cable is used to connect two or more computing devices. The internal wiring of crossover cables reverses the transmission and receive signals. It is widely used to connect two devices of the same type: e.g., two computers or two switches to each other.

In regard to physical appearance, Crossover Ethernet cables are very much similar to regular Ethernet cables. Still, they are different with regard to the order with which the wires are arranged. This type of Ethernet cable is made to connect to network devices of the same kind over Ethernet directly. Crossover cables are mostly used to connect two hosts directly.

**Devices Connectivity:**

| DEVICES | HUB | SWITCH | ROUTER | PC |
|---|---|---|---|---|
| HUB | **CO** | **CO** | **ST** | **ST** |
| SWITCH | **CO** | **CO** | **ST** | **ST** |
| ROUTER | **ST** | **ST** | **CO** | **CO** |
| PC | **ST** | **ST** | **CO** | **CO** |

# Exercise 2.a Demonstration of P2P Network

**Objective:** To demonstrate the Copper Cross-over cabling by designing a Peer to Peer Network

**Components**:

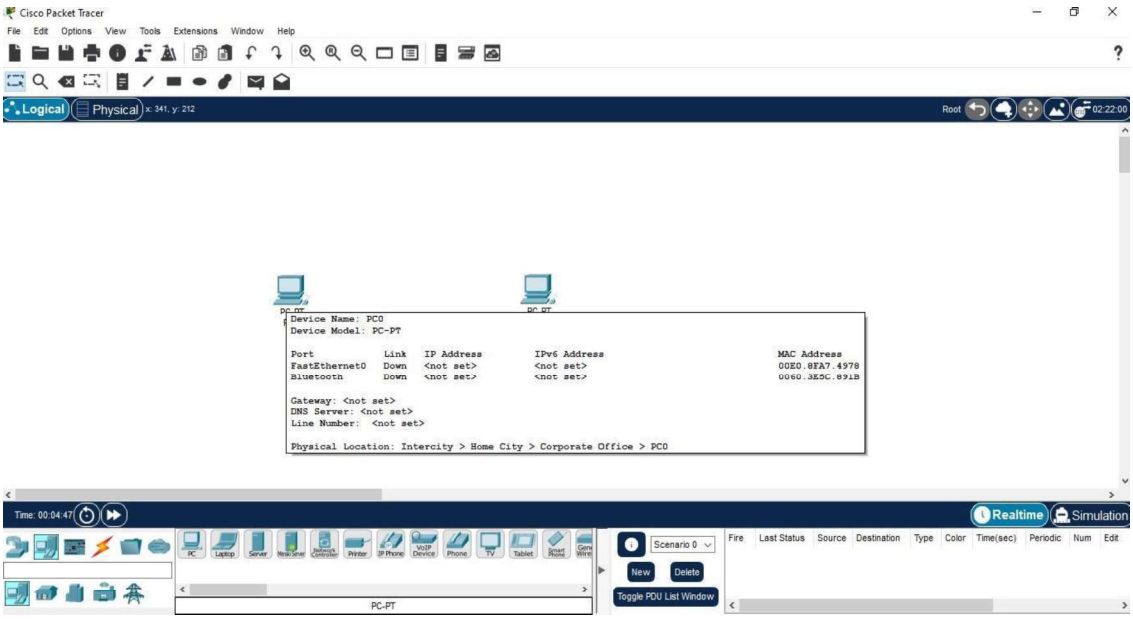
| Devices | Required Nos |
|---|---|
| PCs | 2 |
| Copper Cross – Over Cable | 1 |

**Addressing Table:**

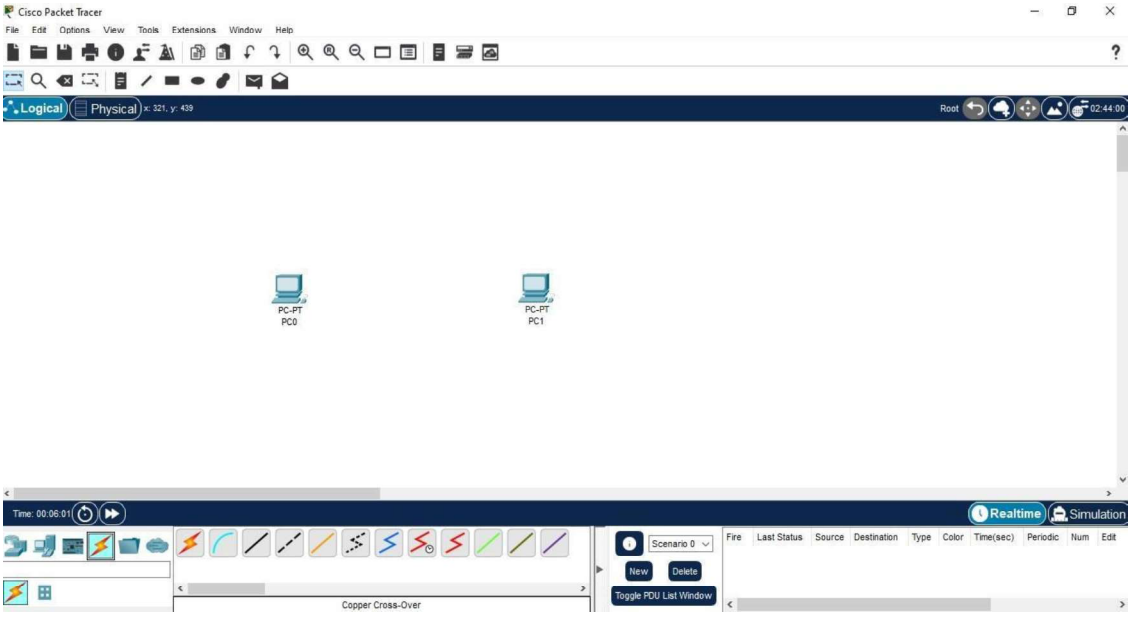
| Device | Interface | IP Address | Subnet Mask |
|---|---|---|---|
| PC0 | Fa0/0 | 192.168.10.1 | 255.255.255.0 |
| PC1 | Fa0/0 | 192.168.10.2 | 255.255.255.0 |

**Procedure:**

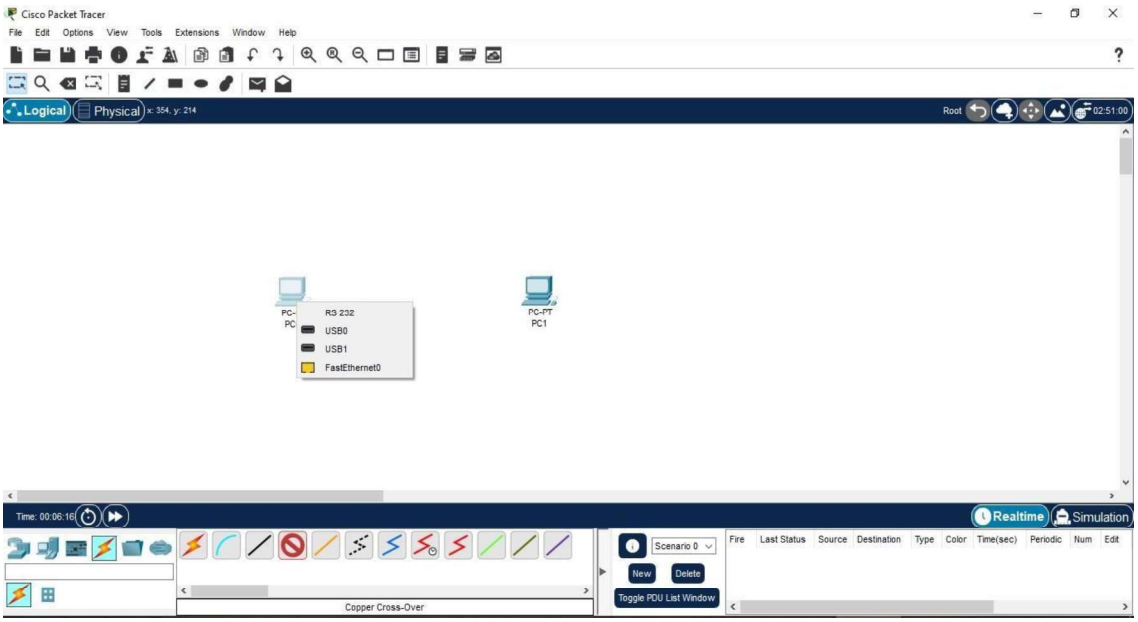
**Step 1:** Drag 2 PCs in the console area. Each PC will have interfaces as shown in the figure.



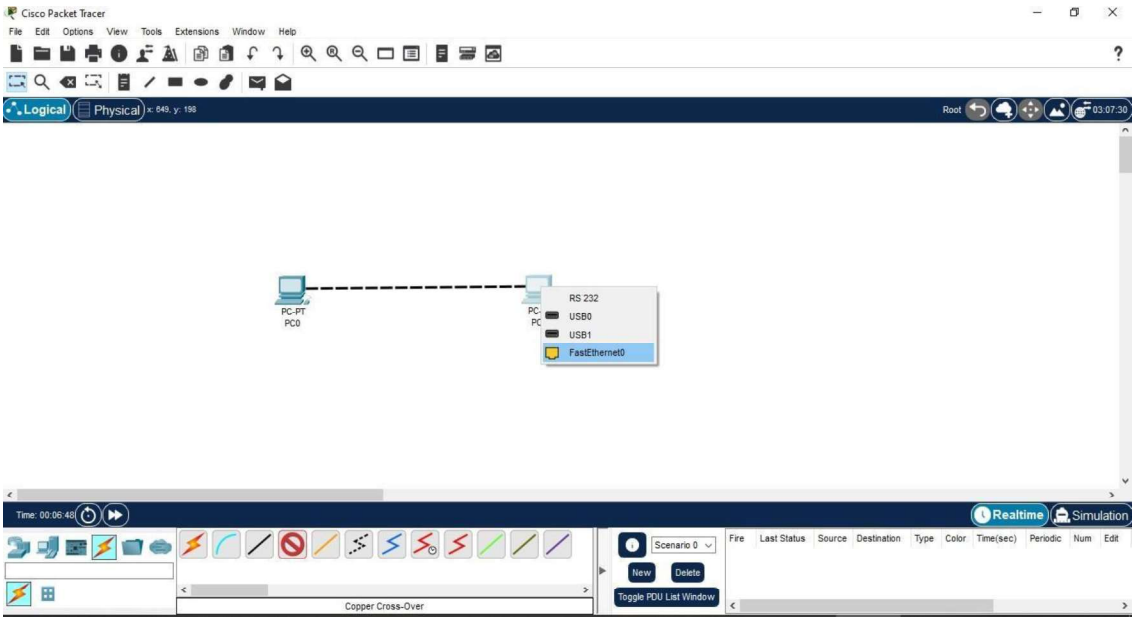
**Step 2:** Select Connectivity & Copper cross-over cable.




**Step 3:** Click on PC0 to get the interface options. Select Fa0/0

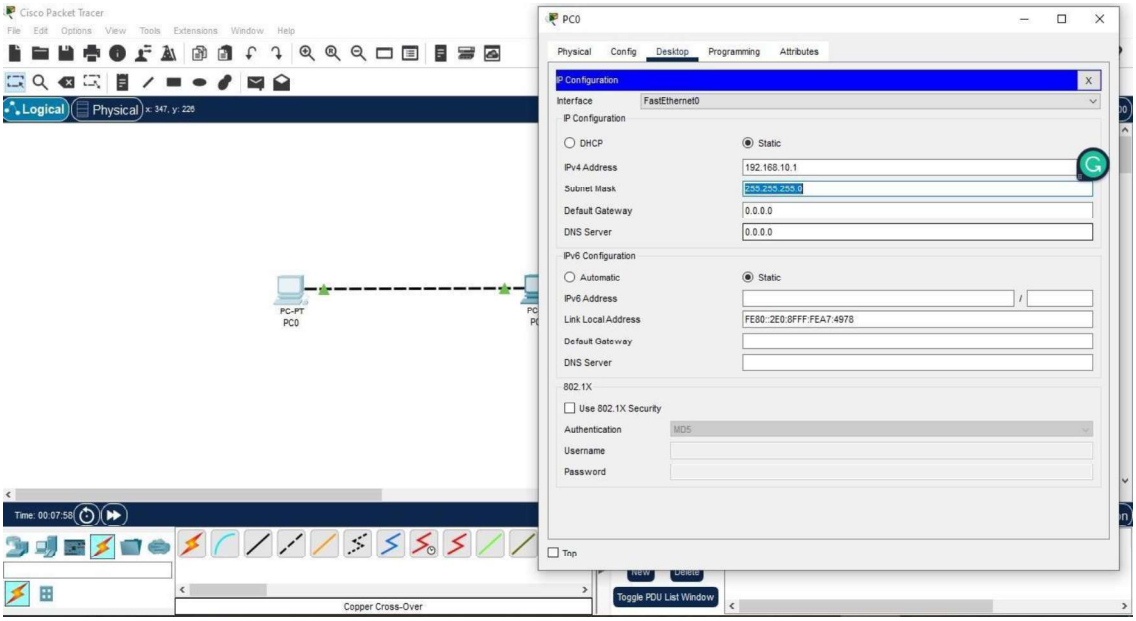


**Step 4:** Click on PC1 to get the interface options and select Fa0/0.

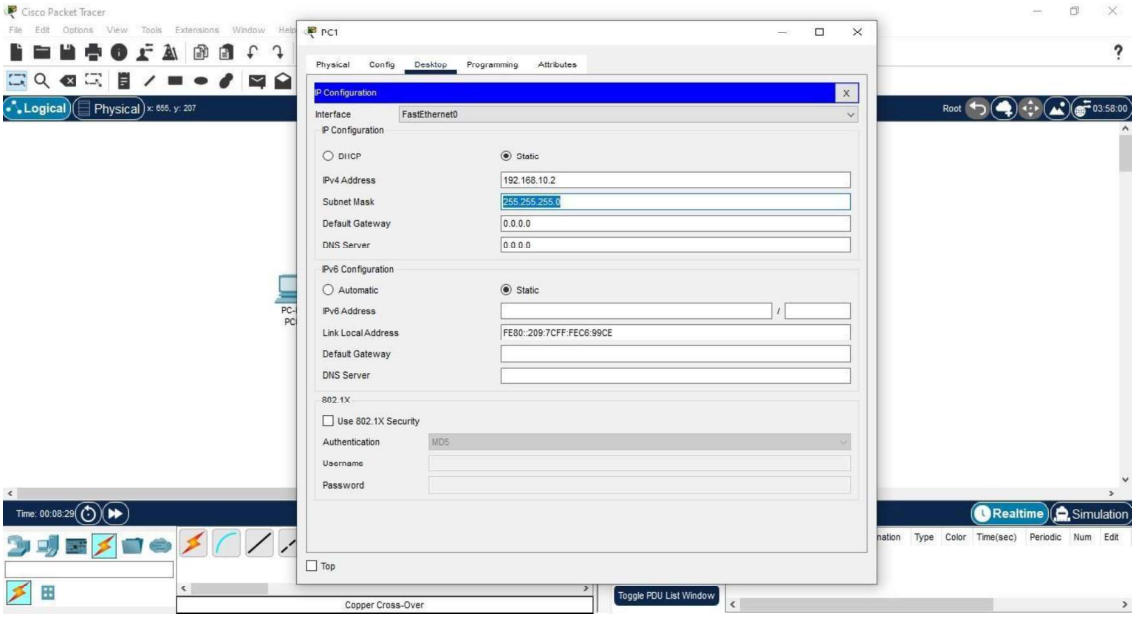



**Step 5**: Now the PCs are physically connected. To establish logical connectivity,

- Click on PC0.
- Select Desktop tab.
- Click on IP Configuration icon.
- Configure as in the following figure

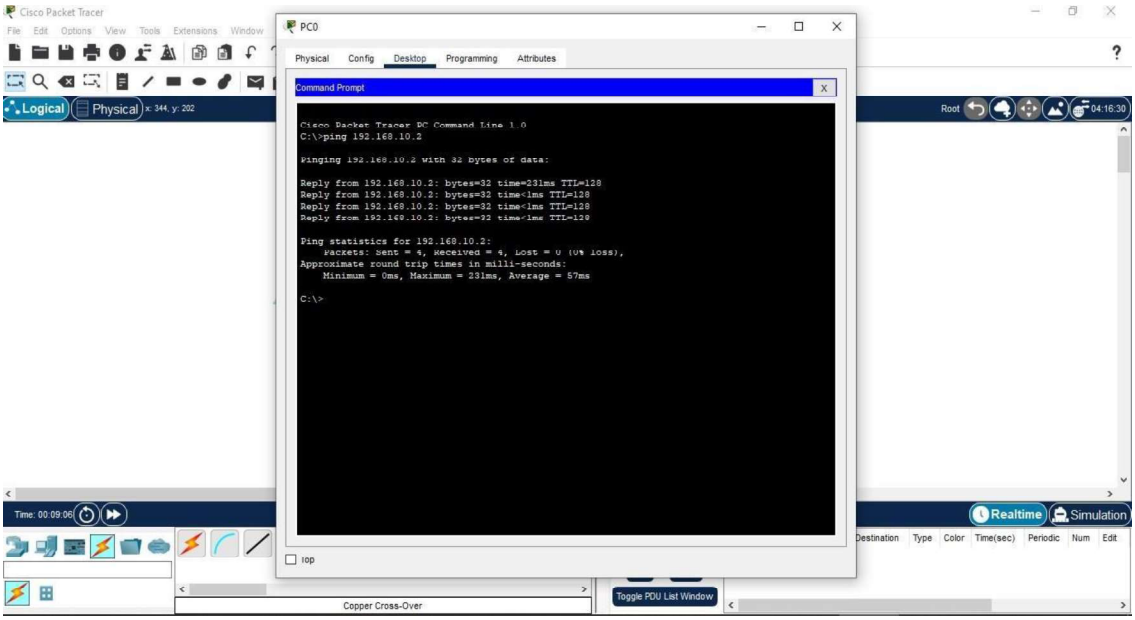


**Step 6:** Configure IP address for PC1 with the same procedure.




**Step 7:** Now both the PCs are physically and logically connected. To check the logical connectivity,

- Click on PC0.
- Select Desktop tab.
- Click on Command Prompt icon.
- Type ping 192.168.10.2 to fetch the output as follows



## Exercise 2.b Demonstration of Simple LAN

**Objective:** To demonstrate the straight through cabling by designing a Local Area Network

**Components**:

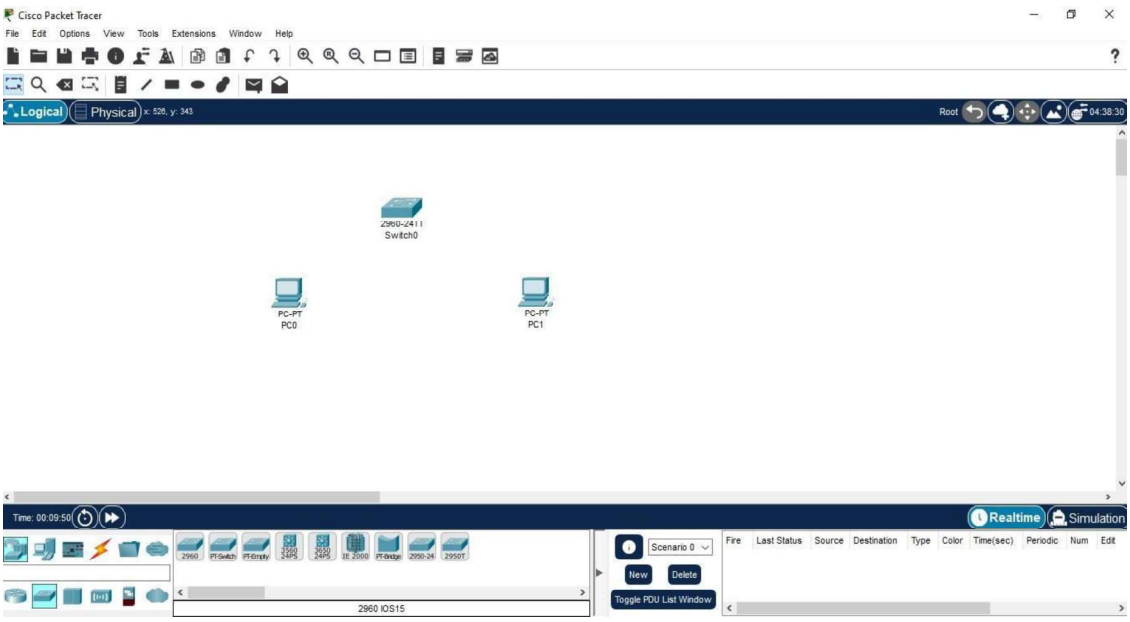
| Devices | Required Nos |
|---|---|
| PCs | 2 |
| Copper Straight – Through Cables | 2 |
| Switch | 1 |

**Addressing Table:**

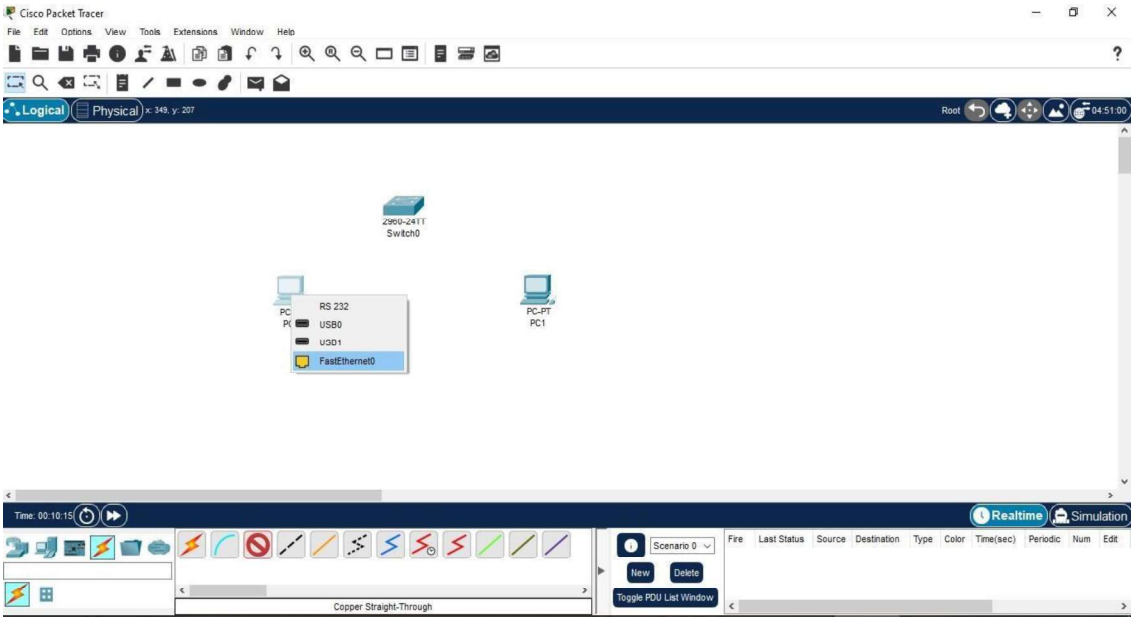
| Device | Interface | IP Address | Subnet Mask |
|---|---|---|---|
| PC0 | Fa0/0 | 192.168.10.1 | 255.255.255.0 |
| PC1 | Fa0/0 | 192.168.10.2 | 255.255.255.0 |

**Procedure:**

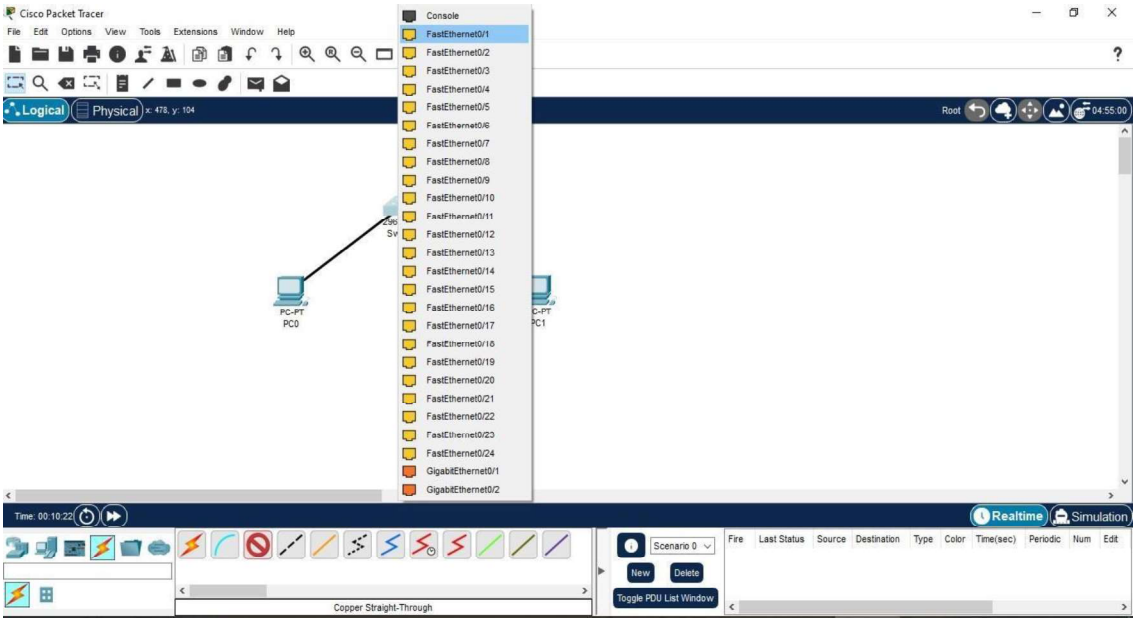
**Step 1:** Drag 2 PCs and a switch in the console area. Each PC will have interfaces as shown in the figure.



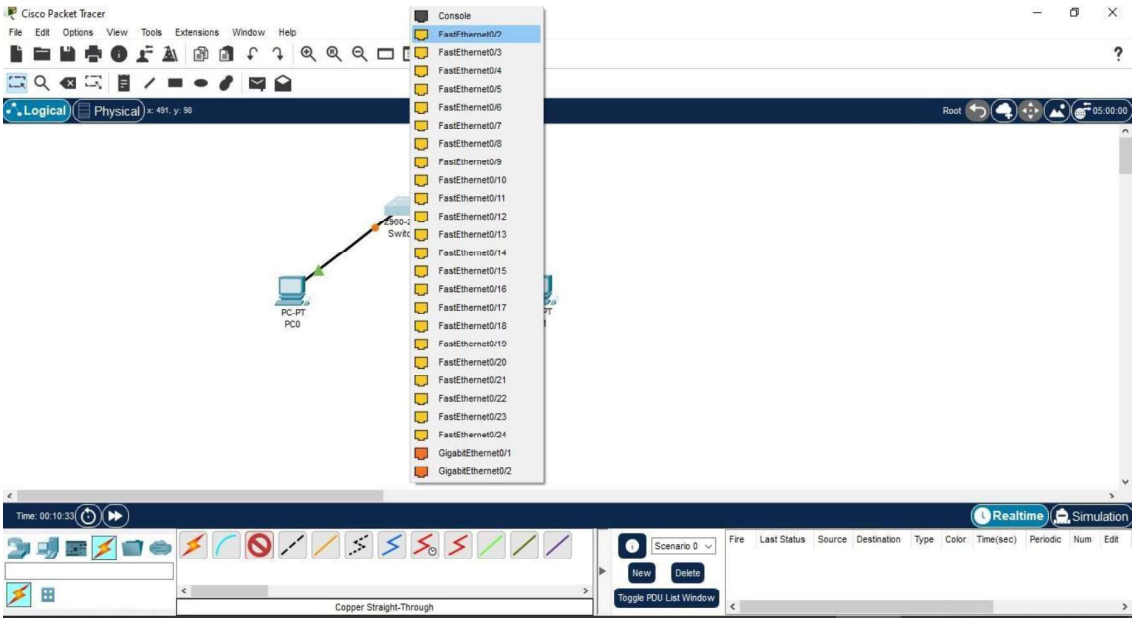
**Step 2:** Select Connectivity & Copper Straight-Through cable. Click on PC0 to get the interface options. Select Fa0/0



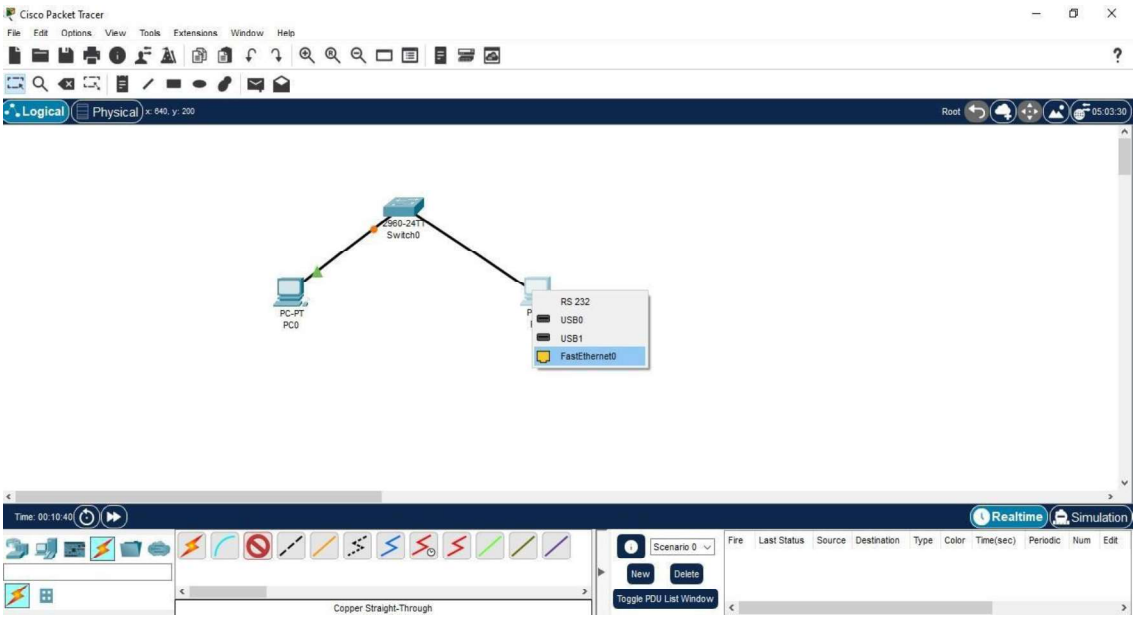

**Step 3:** Click on Switch to get the interface options and select Fa0/0.



**Step 4**: Now PC0 and Switch are physically connected. Again select copper straight-through cable and again click on Switch to get the interface options and select Fa0/1.




**Step 5:** Click on PC1 to get the interface options and select Fa0/0.

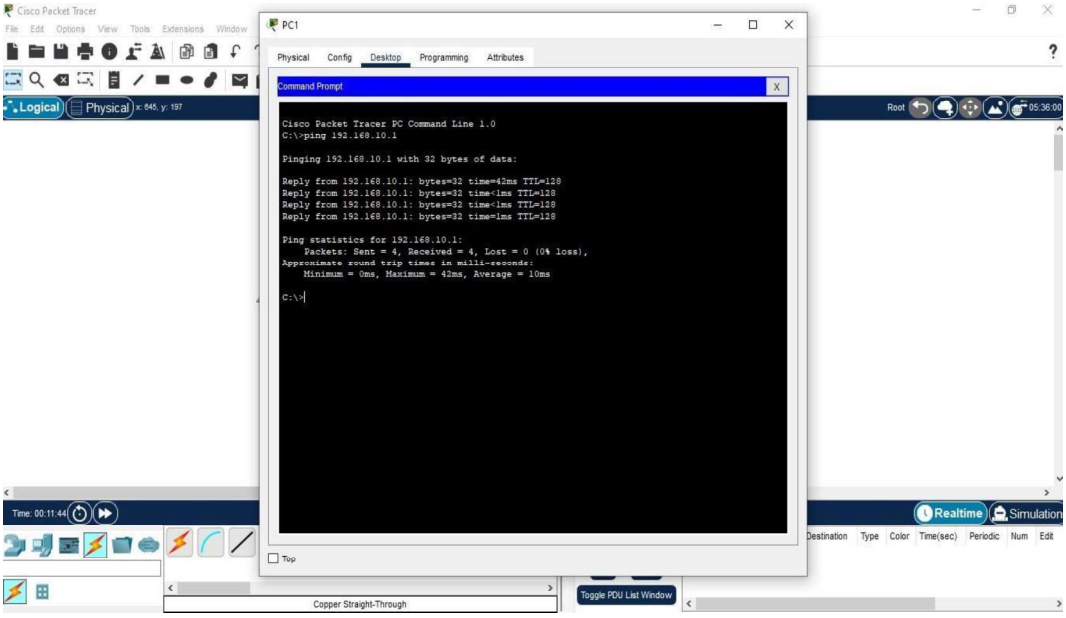


**Step 6:** Now the PCs are physically connected through switch. To establish logical connectivity,

- Click on PC0.
- Select Desktop tab.
- Click on IP Configuration icon.
- Configure the ip address 192.168.10.1 and subnet mask 255.255.255.0
- Repeat the same procedure for PC1 and configure with the ip address 192.168.10.2 and subnet mask 255.255.255.0

**Step 7:** Now both the PCs are physically and logically connected. To check the logical connectivity,

- Click on PC1.
- Select Desktop tab.
- Click on Command Prompt icon.
- Type ping 192.168.10.1 to fetch the output as follows




Result:

Thus the implementation of P2P and LAN is done successfully.