

NETWORKING

SIX WEEKS INDUSTRIAL TRAINING REPORT

Submitted by

Deepak

2820431

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

AT



SCHOOL OF ENGINEERING, DESIGN AND

AUTOMATION

DEPARTMENT OF COMPUTER SCIENCE AND

ENGINEERING

JUNE - JULY 2023

ACKNOWLEDGEMENT

While presenting this report I would like to express my deep sense of gratitude to entire Solitaire staff that was indispensable part of my training giving me unending guidance, inspiration, encouragement and providing me excellent environment throughout my training at Solitaire Infosys Pvt. LTD. The training was an extremely productive; enriching experience, not only technically but also from providing practical skills. I am extremely thankful to Mr. Sham Sunder who had devoted a lot of time in guiding and supervising me during my training. I place my gratitude towards Mr. Sham Sunder for his valuable advice and guidance in carrying out this enjoyable and productive experience, which provided me a great opportunity to search new horizons.

Deepak
2820431

ABSTRACT

The networking course is designed to provide participants with a solid foundation in networking principles, protocols, and technologies. Over the duration of the course, participants will be introduced to key concepts such as network architecture and network design. Through a combination of theoretical instruction and practical hands-on exercises, participants will gain the necessary skills to configure, manage, and maintain computer networks effectively.

The course begins with an introduction to networking fundamentals, including an overview of network models such as the OSI and TCP/IP models. Participants will learn about different network topologies, protocols, cabling and the functions of network devices. As the course progresses, participants will delve into the intricacies of routing protocols such as RIP, OSPF, EIGRP.

Network security is a crucial aspect of the course, covering areas such as virtual private networks (VPNs), DNS server, Email server, NAT, VOIP. Participants will also gain insights into network design methodologies, IP addressing, redistribution and subnetting.

By the end of the course, participants will have developed a comprehensive understanding of networking fundamentals and acquired practical skills to design, configure computer networks. This knowledge and expertise will enable them to pursue careers in network administration, engineering, or security, contributing to the efficient and secure functioning of modern digital infrastructures.

TABLE OF CONTENTS

SNO.	TITLE	PAGE NO.
1.	Introduction	4
2.	Network & Types	5
3.	Ways of transmission in computer network	6
4.	Networking Cables	7-8
5.	Networking Devices	9-12
6.	IP Address	13-14
7.	OSI Model	15-16
8.	Cisco Packet Tracer	17
9.	Networking Devices used in Project	18
10.	Implementation of Project	19-21
11.	Cisco Router Modes	22
12.	Assign IP Address to Switch, Router & PC	23-24
13.	Routing Protocols	25-26
14.	Redistribution	27-28
15.	Voice Over Internet Protocol	29-30
16.	Telecommunication Network	31-32
17.	Secure Shell	33-34
18.	WiFi server	35-37
19.	Subnetting	38-40

INTRODUCTION

Networking is the backbone of modern communication systems, enabling devices and computers to connect and share information with each other. It involves the interconnection of multiple devices, such as computers, smartphones, servers, and other electronic devices, to form a network that allows data to be exchanged and accessed.

In simple terms, think of networking as a system of roads connecting different destinations. Each device, like a computer or a smartphone, is a destination, and the network is the road system that enables these devices to communicate and share data.

Networks can be as small as a home or office network, where devices are connected together to share files and printers, or they can be as vast as the internet, which connects billions of devices worldwide. The internet is the largest and most well-known network, allowing people to access websites, send emails, and engage in various online activities.

Networking relies on protocols, which are a set of rules and standards that govern how data is transmitted and received across the network. One commonly used protocol is the Internet Protocol (IP), which assigns unique addresses to each device on the network, ensuring that data is properly directed to its intended recipient.

Different types of networks exist, including wired and wireless networks. Wired networks use physical cables, like Ethernet cables, to connect devices, while wireless networks use radio waves to transmit data without the need for physical connections.

Overall, networking is all about connecting devices and enabling them to communicate and share information. It plays a crucial role in our daily lives, powering the internet, online communication, and many other applications that rely on the seamless transfer of data between devices.

NETWORK & TYPES

A network refers to a collection of devices (such as computers, servers, printers, and routers) that are connected together to share resources and communicate with each other. These devices can be physically connected using cables or wirelessly connected through Wi-Fi.

There are different types of networks based on their size and geographical coverage:



Local Area Network (LAN): A LAN is a network that covers a small area, such as a home, office, or building. It allows devices within this limited space to share files, printers, and internet connections.

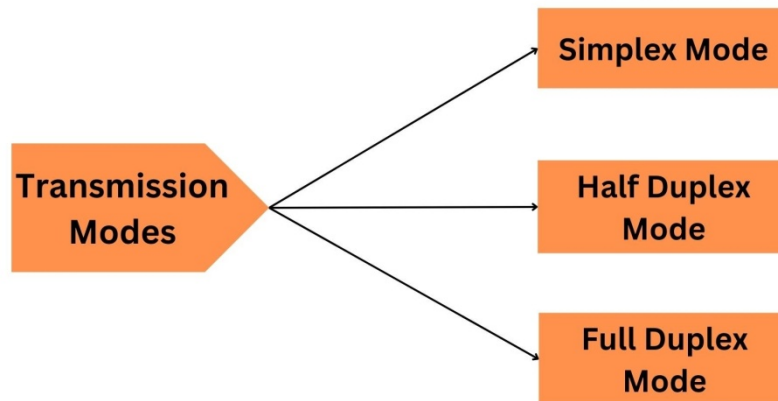
Metropolitan Area Network (MAN): A MAN is a network that spans across a city or town. It connects multiple LANs together, allowing them to share resources and communicate with each other.

Wide Area Network (WAN): A WAN is a network that covers a wide geographical area, such as multiple cities, countries, or even continents. The Internet is the most well-known example of a WAN, connecting networks and devices around the world.

Each type of network serves a different purpose and has varying sizes and coverage areas. LANs are suitable for small-scale networking within a limited space, MANs connect LANs across a city or town, and WANs enable connectivity on a global scale.

WAYS OF TRANSMISSION IN COMPUTER NETWORK

Ways of transmission in computer networks refer to the methods used to send and receive data between devices. The ways of transmission in computer networks: simple mode, half-duplex mode, and full-duplex mode.



Simple Mode: One-way data transmission.

In simple mode, data transmission occurs in only one direction. One device sends the data, and the other device only receives. Example: Radio or television broadcast.

Half-Duplex Mode: Two-way data transmission, but not simultaneously.

In half-duplex mode, data transmission can occur in both directions, but not simultaneously. Devices take turns sending and receiving data. When one device is transmitting, the other device listens and waits for its turn to transmit. Example: Walkie-talkie conversation, Bluetooth.

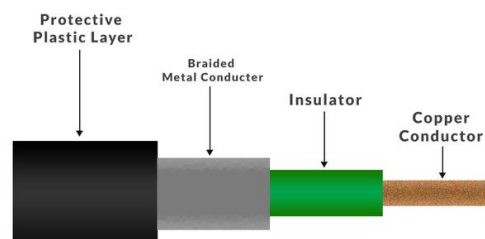
Full-Duplex Mode: Two-way simultaneous data transmission.

In full-duplex mode, data transmission can occur simultaneously in both directions. Both devices can send and receive data simultaneously without having to wait or take turns. Example: Whatsapp chats, telephone conversation.

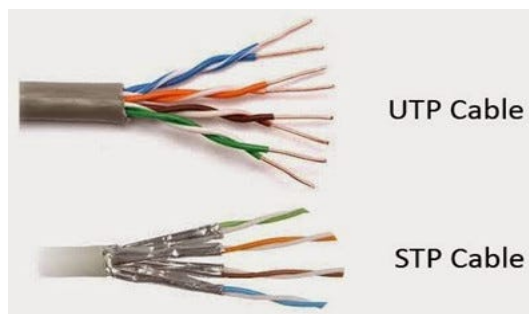
NETWORKING CABLES

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share devices such as printers or scanners. Different types of network cables, such as coaxial cable and twisted pair cables are used.

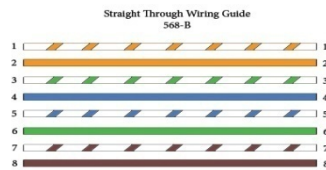
- **COAXIAL CABLE:** Coaxial cables have a central copper conductor that carries the signal. The conductor is surrounded by insulation, which is then covered by a metallic shield (usually made of aluminum or copper) to reduce interference. Finally, there is an outer plastic or rubber covering for protection. Coaxial cables are commonly used for cable television and broadband internet connections.



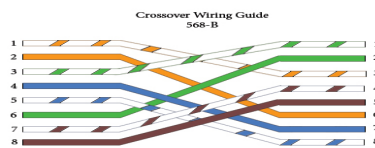
- **TWISTED PAIR CABLE:** Twisted pair cables consist of pairs of copper wires twisted together in a specific pattern. They are widely used in Ethernet networks and telecommunications systems.
 - Shielded Twisted Pair (STP): Shielded Twisted Pair cables have extra protection against interference. STP cables have an additional shielding layer around the twisted pairs of copper wires.
 - Unshielded Twisted Pair (UTP): Unshielded Twisted Pair cables do not have extra protection. They rely on the twisting of the wire pairs to reduce interference.



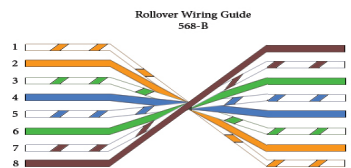
- **Straight-through cable:** Used to connect different types of devices (e.g., computer to switch). Sequence: orange/white, orange, green/white, blue, blue/white, green, brown/white, brown.



- **Crossover cable:** Allows direct connection between similar devices (e.g., computer to computer). Sequence: Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6.



- **Roll-over cable:** Primarily used to connect a computer to a router or network switch for management or configuration purposes. Sequence: Reverse the pin order of each wire in a cable.



- **Fiber optic cable:** Utilizes thin glass or plastic fibers to transmit data using light signals, offering high-speed and long-distance communication.



- **Serial cable:** Connects devices like routers, switches, and modems to computer serial ports for serial communication.



- **Console cable:** Enables a direct connection between a computer and networking equipment (e.g., router or switch) for management and configuration purposes.

NETWORKING DEVICES

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, etc.

➤ LAN Card

A LAN card, also known as a network interface card (NIC) or Ethernet card, is a hardware device that enables a computer to connect to a local area network (LAN). It provides the physical interface between the computer and the network, allowing data to be transmitted and received over the network. The MAC address is indeed stored in the LAN card itself.



➤ REPEATER

A repeater operates at the physical layer. It is a hardware component that is used to boost up signals and also receive signal and retransmits it at higher frequency. According to the types of signals that they regenerate, repeaters can be classified into two categories:

- **Analog Repeaters** : It can only amplify the analog signal.
- **Digital Repeaters** : It can reconstruct a distorted signal.



➤ HUB

A hub is a network device that connects multiple devices in a local area network (LAN). It operates at the physical layer of the network and is primarily used for signal distribution. It performs broadcasting and LAN device which connects computer together and works on half duplex. It does not understand MAC address. . In HUB, there is 7 to 12 port. The speed is same as cable speed or connection speed.



In networking, there are primarily three types of hubs:

- **Active HUB:** It is also known as Multiport Repeater. Power is required for initiating and it detects error. It also amplifies data and regenerates the data.
- **Passive HUB:** It does not require power for initiating and it sends data as it is.
- **Intelligent HUB:** It is a manageable hub and power required. It detects error and correct it upto certain limits.

➤ SWITCH

A switch is a multiport bridge with a buffer and a design that can boost its efficiency and performance. A switch is a data link layer device. It is a LAN device and a central device which is used in network for connecting devices. The number of ports are more than hub. It has max 24 ports. It understand MAC address and work on full duplex mode. The speed of switch is double than connection speed.



Based on their configuration types, switches can be categorized into two main types:

- **Unmanaged Switch:**

Unmanaged switches are the most basic type of switch and are typically used in small home or office networks. They are plug-and-play devices that require no configuration or management. Unmanaged switches operate with default settings and cannot be customized.

- **Managed Switch:**

Managed switches offer advanced configuration and management capabilities, making them suitable for larger networks and enterprise environments. They provide a range of features and options that allow network administrators to have greater control over the network.

➤ **BRIDGE**

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol.

➤ **GATEWAY**

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

➤ **FIREWALL**

A firewall device is a crucial component of network security that monitors and filters network traffic based on predefined rules. It acts as a barrier between networks, preventing unauthorized access and protecting against threats. Firewalls enforce security policies, perform traffic inspection, and can include features such as NAT, intrusion detection/prevention, and VPN support. They play a vital role in enhancing network security and protecting sensitive data from unauthorized access or malicious activities.

➤ ROUTERS

A router is a network device that forwards information packets among PC networks. Routers perform traffic routing functions on the Internet. Data sent over the Internet, such as a website or email, is in the form of data packets. Data travels through these interfaces in the network. Ports and interfaces are identified by their name and number. Different types of Ports are mentioned below:

- **Serial Port:** A serial port is used for serial communication and is typically used for connecting to external devices like modems or other routers. Serial ports are used for wide area network (WAN) connectivity in older router models. Serial cable is used in it.
- **Console Port:** The console port provides a direct management interface for configuring and monitoring the router. It is used to establish a connection between a computer or terminal and the router for accessing the command-line interface (CLI) or other management interfaces. Console cable is used in it.
- **Fast Ethernet Port:** Fast Ethernet ports are used for connecting devices within a local area network (LAN). These ports provide fast Ethernet connectivity, typically at speeds of 100 Mbps. They allow the router to connect to computers, switches, or other networking devices in the local network. Straight cable is used in it.
- **Auxiliary Port:** The auxiliary port, also known as the AUX port, is an auxiliary communication port that allows external devices, such as modems or other networking equipment, to connect to the router for remote management or troubleshooting purposes. Straight cable is used in it.



IP ADDRESS

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network. Typically assigned by an internet service provider (ISP), an IP address is an online device address used for communicating across the internet. The internet needs a way to differentiate between different computers, routers, and websites.

There are two versions of IP addresses that are commonly used on the internet: IPv4 and IPv6.

IPv4	IPv6
IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.
It does not provide encryption and authentication.	It provides encryption and authentication.

Types of IP addresses

- **Private IP addresses:** Each device connected to a home network or a private network carries a private IP address. Private IP addresses are only used on an internal network.
- **Public IP addresses:** An ISP assigns these addresses, which enable a router to communicate with the internet or an outside network. Public IP addresses cover the entire network, meaning multiple devices sharing the same internet connection will also share the same public IP address.
- **Dynamic IP addresses:** These IP addresses are constantly changing and a new dynamic IP address is assigned to a device every time it connects to the internet.
- **Static IP addresses:** Unlike dynamic IP addresses, static IP addresses never change once they're assigned by the network. A static IP address ensures that all websites and email addresses associated with a certain web server.

In the IPv4 IP address space, there are five classes: A, B, C, D and E. Each class has a specific range of IP addresses. Primarily, class A, B, and C are used by the majority of devices on the Internet. Class D and class E are for special uses.

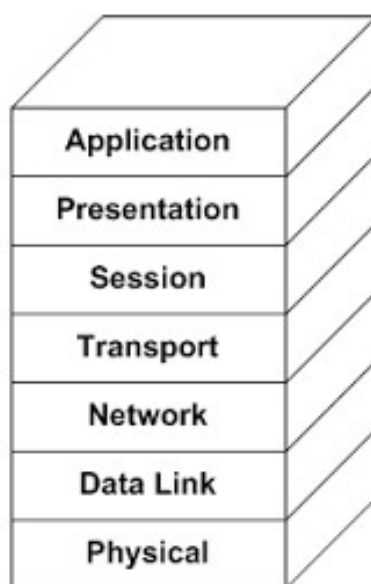
Class	Network Bits	Host Bits	Range	Subnet Mask
Class A	8	24	1-126	255.0.0.0
Class B	16	16	128-191	255.255.0.0
Class C	24	8	128-191	255.255.255.0
Class D	Used in multicasting	Used in multicasting	224-239	-
Class E	Used for research	Used for research	240-254	-

OSI MODEL

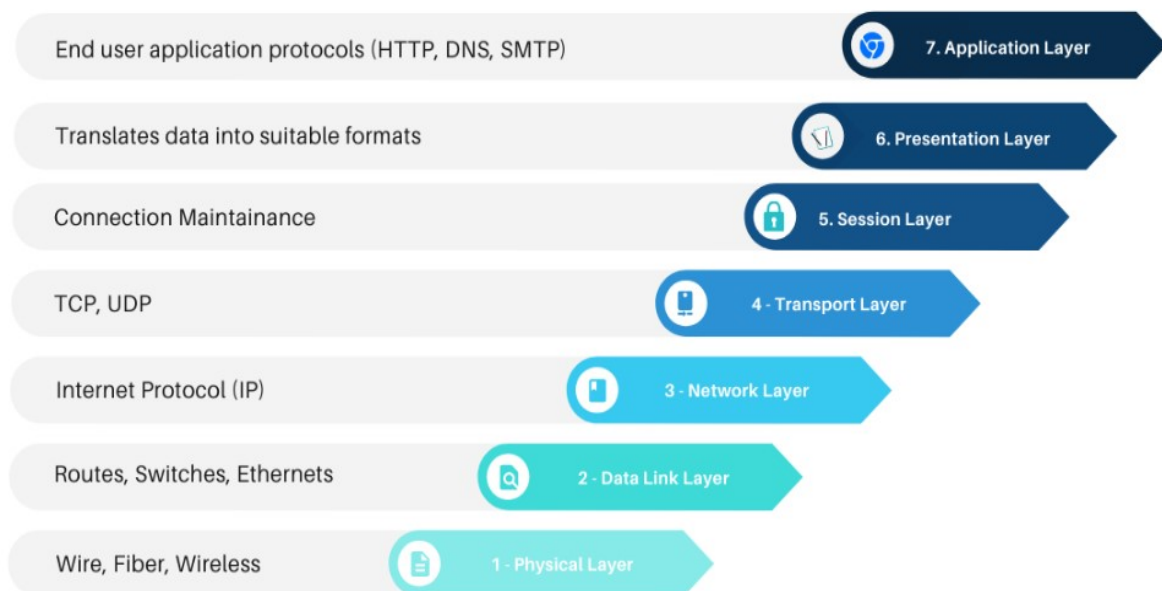
- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

➤ 7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:



- **Physical Layer:** Deals with the physical transmission of data over the network.
- **Data Link Layer:** Manages reliable communication between directly connected devices.
- **Network Layer:** Handles addressing and routing of data packets across multiple networks
- **Transport Layer:** Ensures reliable delivery of data segments between endpoints.
- **Session Layer:** Establishes, manages, and terminates communication sessions between applications.
- **Presentation Layer:** Handles data formatting and translation for different applications.
- **Application Layer:** Enables direct interaction between user applications and the network.



CISCO PACKET TRACER

Cisco Packet Tracer is a software tool developed by Cisco Systems that allows users to design, configure, and simulate computer networks. It provides a virtual environment where users can create network topologies by adding devices such as routers, switches, PCs, and servers. With Packet Tracer, users can connect these devices, configure their settings, and simulate network operations.

Packet Tracer is widely used in educational settings, such as classrooms and network training programs, as it helps students learn and practice networking concepts. It allows users to visualize and understand how networks work by providing a hands-on experience in a safe and controlled environment. Users can experiment with different network configurations, test the functionality of devices, and simulate network behaviors.

The software supports a range of networking protocols and features, allowing users to explore various networking scenarios and troubleshoot network issues. Overall, Cisco Packet Tracer serves as a valuable tool for learning, testing, and gaining practical experience in the field of computer networking.

Cisco Packet Tracer



Cisco Packet Tracer is used for projects because it provides a virtual environment to design, test, and learn about computer networks, allowing project teams to gain hands-on experience, troubleshoot network issues, and collaborate effectively without the need for physical equipment.

NETWORKING DEVICES USED IN PROJECT

In a networking project using Cisco Packet Tracer, a wide range of devices can be used to create and simulate network environments. Here are some common devices used in such projects:

Routers: Routers are essential devices in network projects. They connect different networks together, handle data routing, and facilitate communication between devices.



Switches: Switches are used to connect multiple devices within a network, allowing them to communicate with each other. They enable efficient data transfer within a local network.



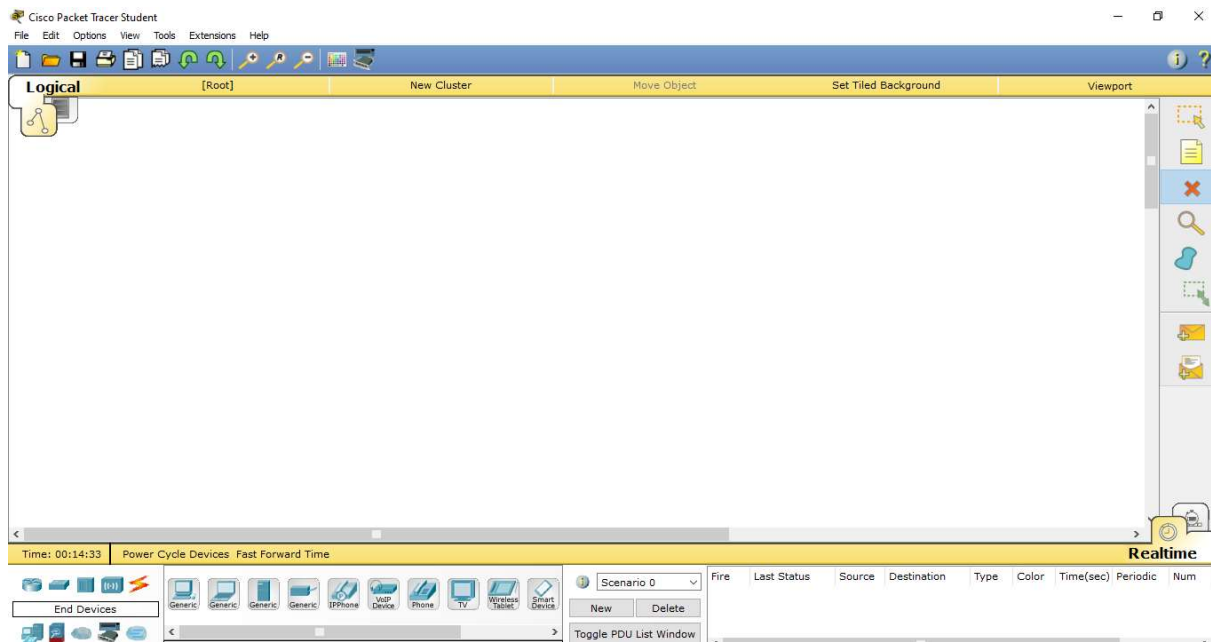
PCs: PCs (Personal Computers) are used to simulate end-user devices in the network. They can represent workstations, laptops, or any other devices that connect to the network.



IMPLEMENTATION OF PROJECT

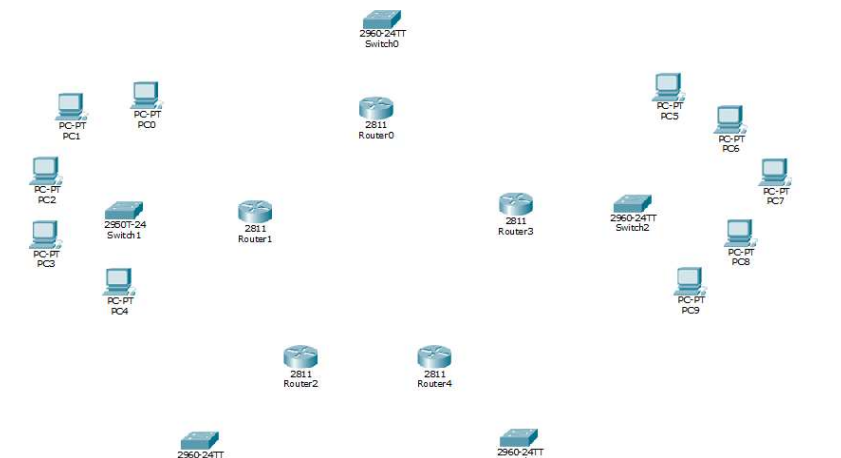
Step 1: Download Cisco Packet Tracer and install the setup.

Step 2: After the installation procedure has completed this display (below) will appear when you run the Cisco Packet Tracer-Start the application.



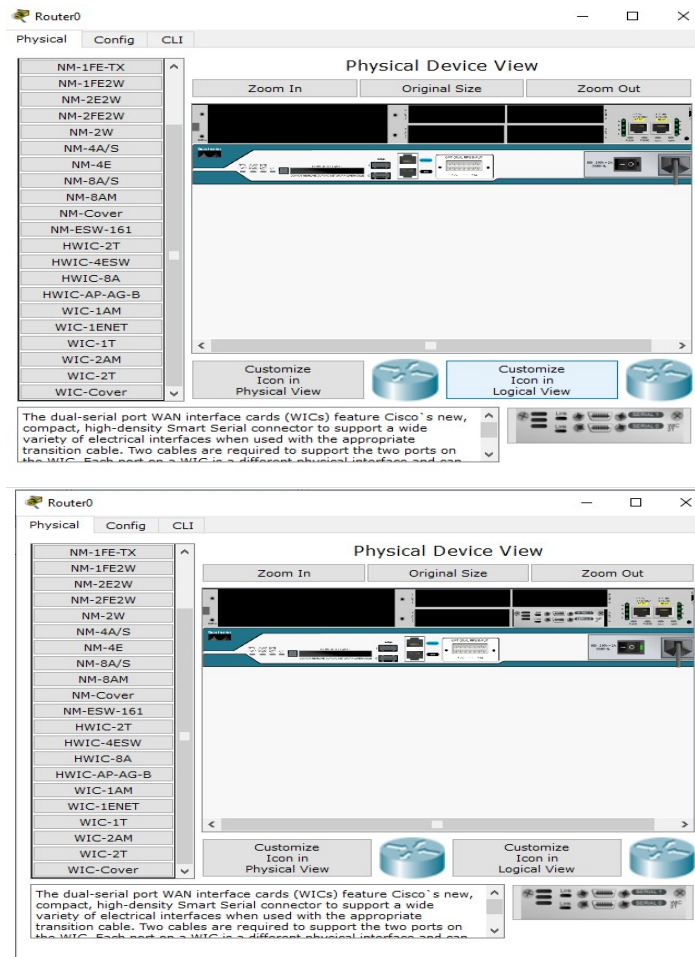
Step 3:

- From the bottom toolbar, click on router and select router 2811.
- Also click on switch and selects 2960 switch.
- Now, click on 'End Devices' and select 'PC' and then click on the screen.

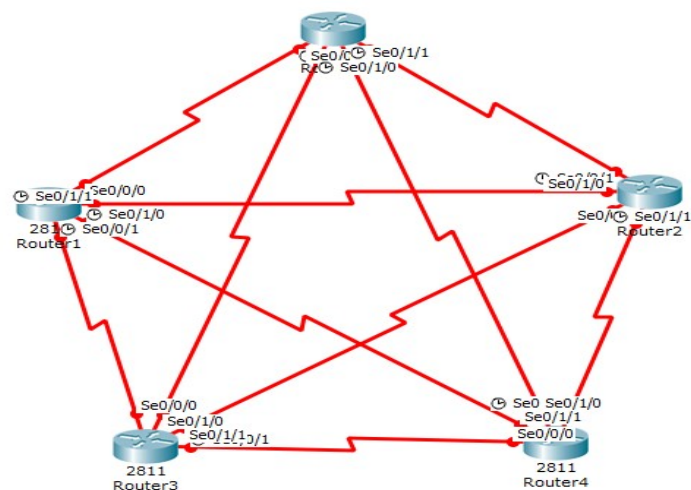


Step 4:

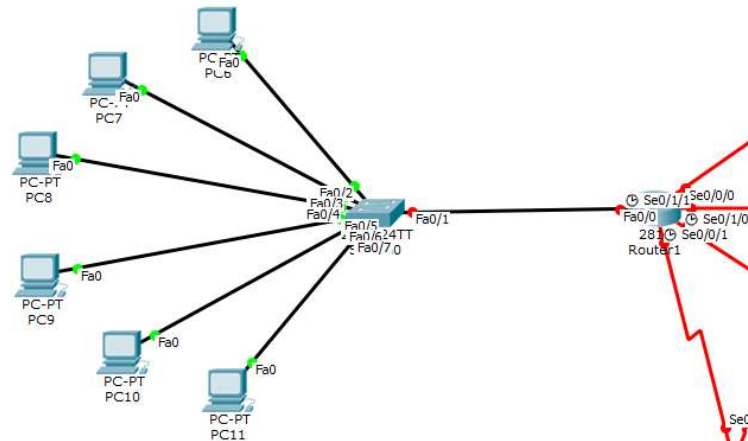
- Connect routers and switches by cable.
- For adding ports in router, click on the router, off the router by clicking on the button and then add the WIC-2T port into the empty port (which is black in color) by dragging it from the left section of the screen. And then again turn on the button by clicking on the same button.



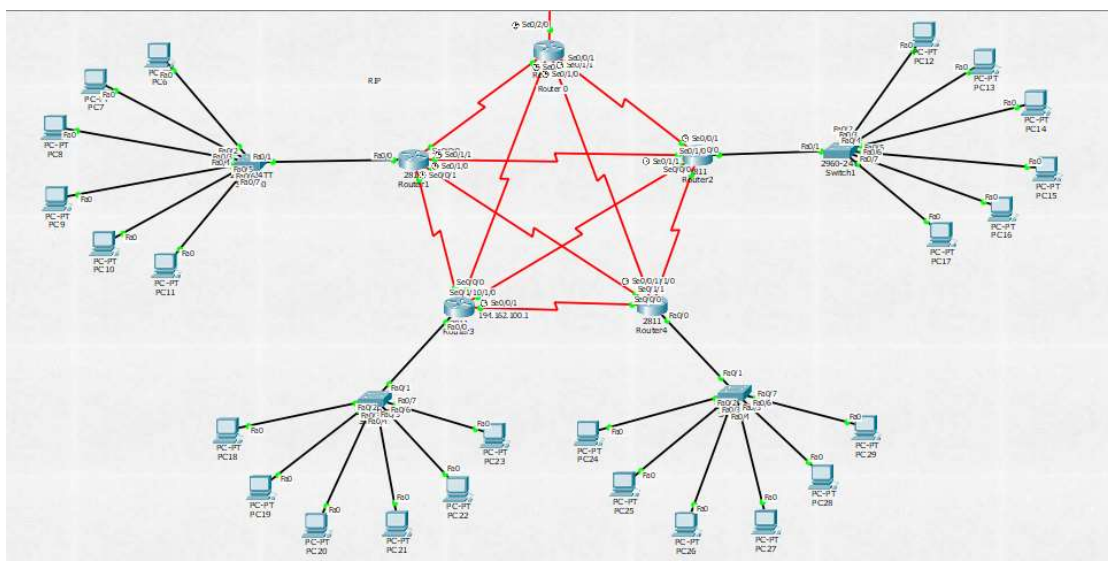
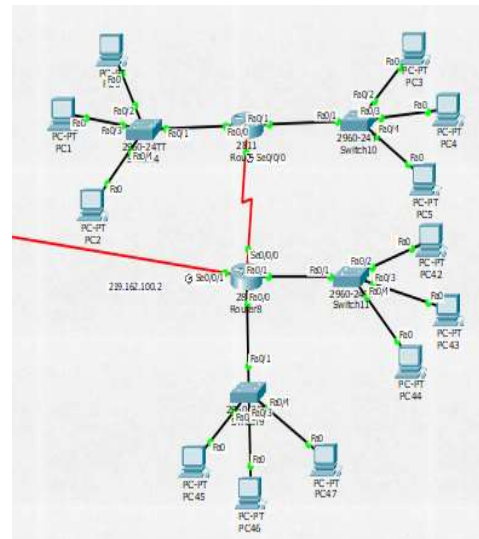
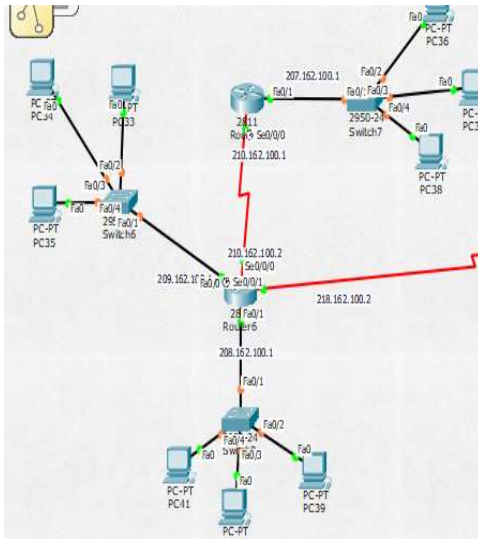
- Now, connect the routers with serial cable.



- Connect the switch with router and PC using straight cable.



- Now, implement cable on the whole network.



CISCO ROUTER MODES

A router is a layer 3 device used to forward packets from one network to another. It forwards the packet through one of its ports on the basis of destination IP address and the entry in the routing table. By using a routing table, it finds an optimized path between the source and destination network.

Let's discuss the Cisco router's different modes.

Modes of router –

There are mainly 5 modes in the router:

1. User execution mode –

As soon as the interface up message appears and press enter, the router> prompt will pop up. This is called user execution mode. This mode is limited to some monitoring commands.

2. Privileged mode –

As we type enable to user mode, we enter into Privileged mode where we can view and change the configuration of the router. Different commands like show running-configuration, show IP interface brief, etc can run on this mode which is used for troubleshooting purposes. Here commands are sh run, sh history, write and so on.

3. Global configuration mode –

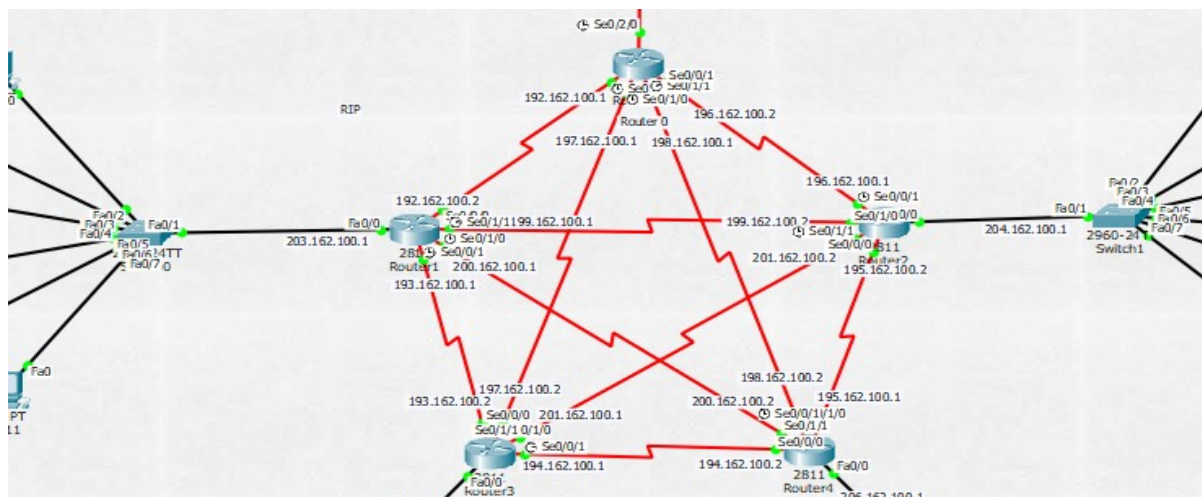
As we type configure terminal to the user mode, we will enter into the global configuration mode. Commands entered in these modes are called global commands and they affect the running configuration of the router. In this mode, a different configuration like making a local database on the router by providing username and password can set enable and secret password, etc. Here commands can execute with do such as do sh run, do write.

Configuration –

```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#|
```


ASSIGN IP ADDRESS TO SWITCH, ROUTER AND PC

Assigning the IP address is the first step while creating a network in packet tracer. Before proceeding with any other configuration, we must assign the appropriate IP address and design the correct IP addressing scheme for the network.



- Click on Router, then on CLI.
- Go to the global configuration mode, and type slot/ port or interface Fast Ethernet 0/0 (or interface fa0/0).
- Now configure an IP address and subnet mask then give “no shutdown” command.
- Carefully configure IP address with proper interfaces to switch and router.

```
Router(config-if)#
Router(config-if)#int se0/1/1
Router(config-if)#ip add 199.162.100.1 255.255.255.0
Router(config-if)#no sh

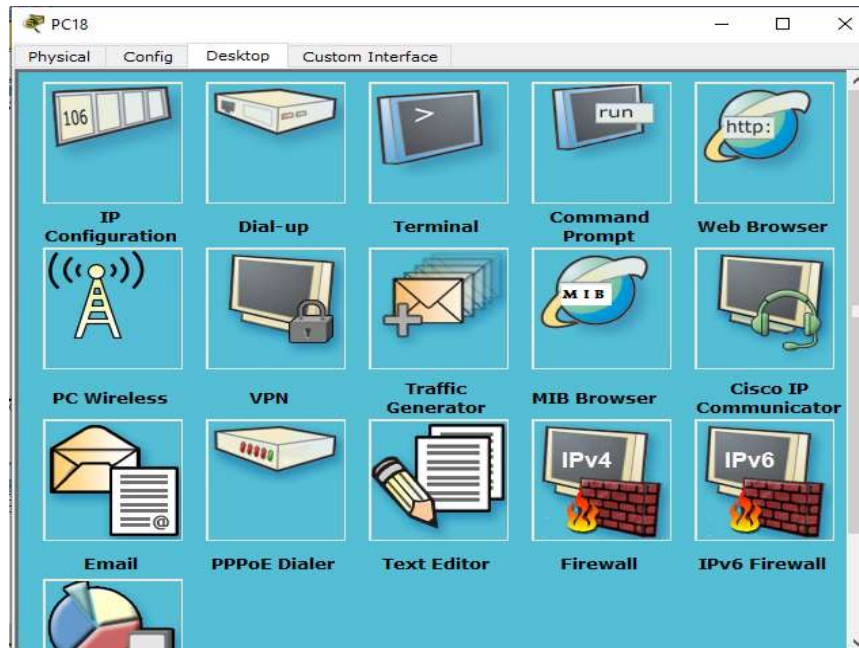
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Router(config-if)#
Router(config-if)#
Router(config-if)#int se0/1/0
Router(config-if)#ip add 200.162.100.1 255.255.255.0
Router(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#
Router(config-if)#int se0/0/1
Router(config-if)#ip add 193.162.100.1 255.255.255.0
Router(config-if)#no sh

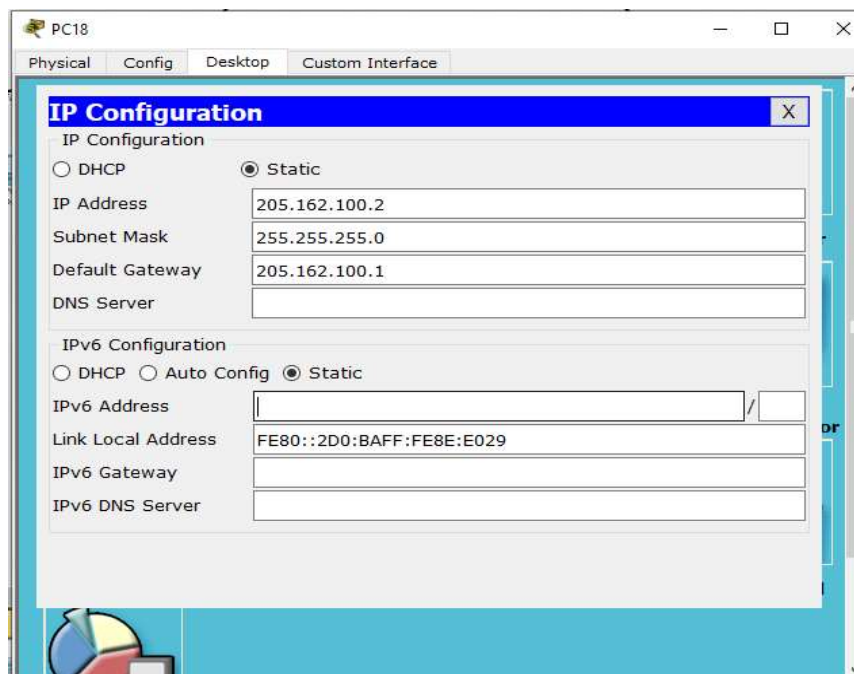
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#
Router(config-if)#int fa0/0
Router(config-if)#ip add 203.162.100.1 255.255.255.0
Router(config-if)#no sh
```


CONFIGURE PC IP ADDRESS

To configure the IP address on a PC, laptop, or server, we have to open the IP configuration utility provided in the packet tracer.



To assign the static IP address, we will select the static option available and then we will configure the IP address manually.



If we have configured the devices with the correct IP addresses then we can further develop our network in the packet tracer.

ROUTING PROTOCOLS

Routing is the process of forwarding network traffic from one network location to another. It involves making decisions about the best path for data packets to reach their destination based on network topology and routing protocols.

A routing protocol is a set of rules and algorithms that routers use to communicate and exchange information about network topology, reachability, and network conditions. These protocols enable routers to learn about available paths, make routing decisions, and update their routing tables to determine the most efficient routes for forwarding data packets.

In simple terms, routing is like finding the best directions to reach a destination in a network, and routing protocols are the rules and methods used by routers to share information and decide the most efficient paths for data to travel through the network.

RIP (Routing Information Protocol):

- RIP is a distance-vector routing protocol that uses hop count as the metric to determine the best path.
- It supports small to medium-sized networks and is easy to configure.
- RIP sends routing updates periodically (by default, every 30 seconds) to its neighboring routers.
- It has a maximum hop count limit of 15, making it suitable for small networks.
- Command use in RIP:

```
Router(config)#router rip
Router(config-router)#net 211.162.100.2
Router(config-router)#net 219.162.100.2
Router(config-router)#net 214.162.100.1
Router(config-router)#net 216.162.100.1
```

OSPF (Open Shortest Path First):

- OSPF is a link-state routing protocol that calculates the shortest path based on the cost assigned to each link.
- It supports large-scale networks and is widely used in enterprise environments.
- OSPF routers exchange link-state information, including the state of their interfaces, with neighboring routers.
- OSPF allows for the use of different metrics, such as bandwidth, delay, and reliability, for path selection.
- Command use in OSPF:

```
Router(config)#router ospf 10
Router(config-router)#net 210.162.100.2 0.0.0.255 area 1
Router(config-router)#net 209.162.100.1 0.0.0.255 area 1
Router(config-router)#net 218.162.100.2 0.0.0.255 area 1
Router(config-router)#net 208.162.100.1 0.0.0.255 area 1
```

EIGRP (Enhanced Interior Gateway Routing Protocol):

- EIGRP is a hybrid routing protocol that combines features of both distance-vector and link-state protocols.
- EIGRP uses a composite metric that includes bandwidth, delay, reliability, and other factors for path calculation.
- It supports automatic summarization and load balancing across multiple paths.
- EIGRP uses a neighbor discovery process and sends partial or incremental updates when changes occur in the network.
- Command use in EIGRP:

```
Router(config)#router eigrp 10
Router(config-router)#net 192.162.100.2
Router(config-router)#net 199.162.100.1
Router(config-router)#net 193.162.100.1
Router(config-router)#net 200.162.100.1
Router(config-router)#net 203.162.100.1
```

REDISTRIBUTION

Redistribution in a computer network refers to the process of sharing routing information between different routing protocols. It is necessary when there are multiple routing protocols being used in a network, and routers need to understand how to forward data between them.

Think of routing protocols as languages that routers use to communicate with each other and exchange information about the best paths to send data. Redistribution allows routers speaking different "languages" (i.e., different routing protocols) to understand each other's information.

When redistribution occurs, routers are configured to translate the routing information from one protocol into another, so that all routers in the network can have a complete and consistent view of the available paths. This helps ensure that data is correctly routed to its destination.

Here is a general overview of the redistribution process:

- **Identify the routing protocols:** Determine the routing protocols that are currently being used within the network and the ones that need to be redistributed.
- **Configure redistribution:** Configure the routers that will be responsible for redistributing the routing information. This typically involves specifying the source routing protocol and the destination routing protocol for redistribution.
- **Define redistribution policies:** Define policies that determine which routes should be redistributed and how they should be redistributed. These policies can include filtering specific routes based on certain criteria or manipulating metric values.
- **Enable redistribution:** Activate the redistribution process on the configured routers. This allows the routers to exchange routing information between the different protocols.
- **Verify and monitor:** Monitor the network to ensure that the redistribution process is functioning as intended. Verify that the redistributed routes are being advertised and received correctly by the routers.

■ CONFIGURE REDISTRIBUTION ON ROUTER

- When router's one interface is operating RIP and other interface is operating EIGRP and OSPF.

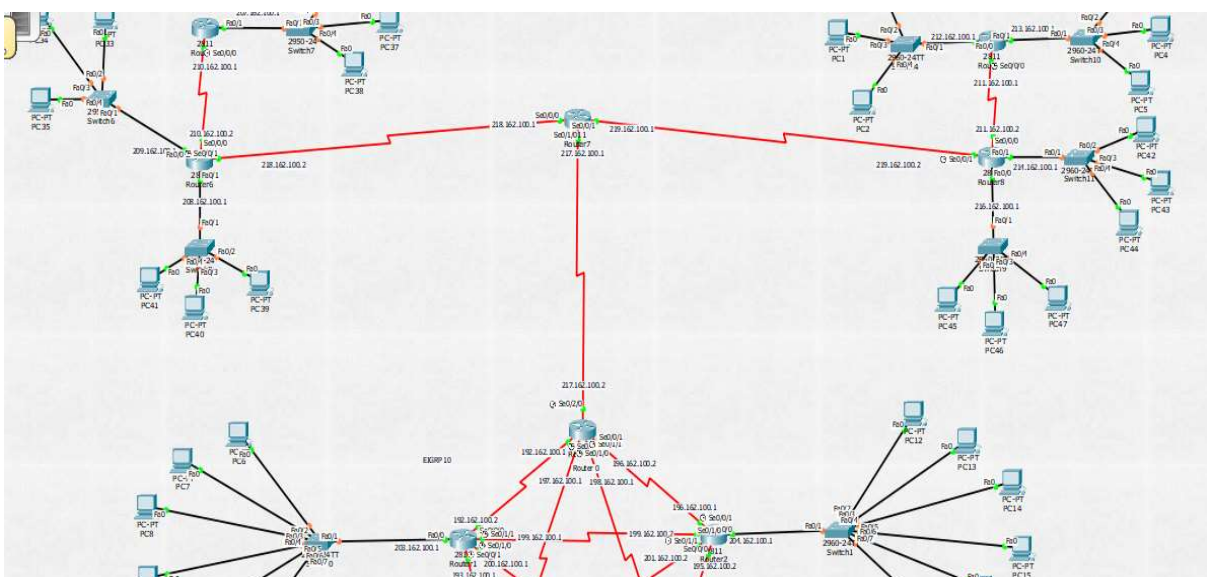
```
router rip
  redistribute eigrp 10 metric 1
  redistribute ospf 10 metric 1
  network 219.162.100.0
```

- When router's one interface is operating OSPF and other interface is given a EIGRP and RIP.

```
router ospf 10
  log-adjacency-changes
  redistribute rip subnets
  redistribute eigrp 10 subnets
  network 218.162.100.0 0.0.0.255 area 1
```

- When router's one interface is operating EIGRP and other interface is given a OSPF and RIP.

```
router eigrp 10
  redistribute rip metric 1 0 100 100 100
  redistribute ospf 10 metric 1 100 100 100 100
  network 217.162.100.0
```



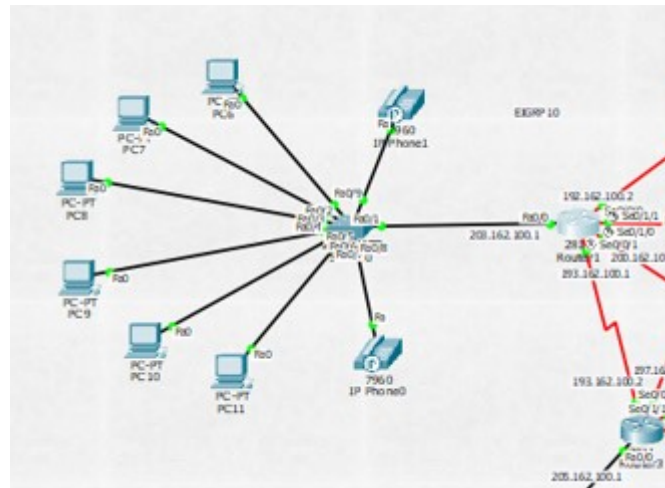
VOICE OVER INTERNET PROTOCOL

VoIP (Voice over Internet Protocol) is a technology that allows voice communication to be transmitted over an IP-based network, such as the internet or a local area network (LAN). Instead of using traditional phone lines, VoIP converts voice signals into digital data packets and sends them over the network.

To configure the voice over internet protocol, the steps are given below.

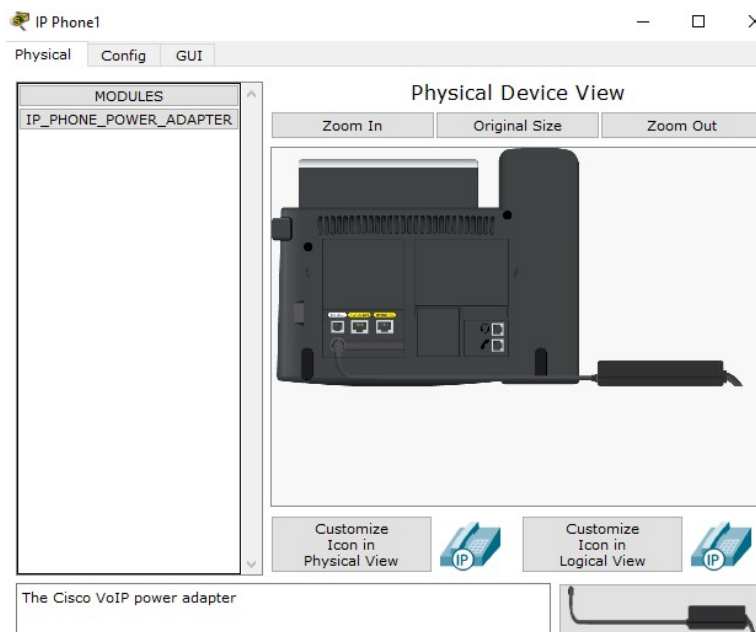
Step 1:

From the bottom toolbar, click on end devices and selects IPphone and connects it with straight cable.



Step 2:

Now, go to physical mode and put the power adapter.



Step 3:

- Go to router and put these commands:

```
Router(config)#ip dhcp pool simran
Router(dhcp-config)#net 208.162.100.0 255.255.255.0
Router(dhcp-config)#default-router 208.162.100.1
Router(dhcp-config)#option 150 ip 208.162.100.1
Router(dhcp-config)#telephony-service
Router(config-telephony)#max-ephone 2
Router(config-telephony)#max-dn 2
Router(config-telephony)#ip source 208.162.100.1 port 2000
Router(config-telephony)#auto assign 1 to 2
Router(config-telephony)#ephone-dn 1
Router(config-ephone-dn)%%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed
state to up

Router(config-ephone-dn)#num 100
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)%%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed
state to up

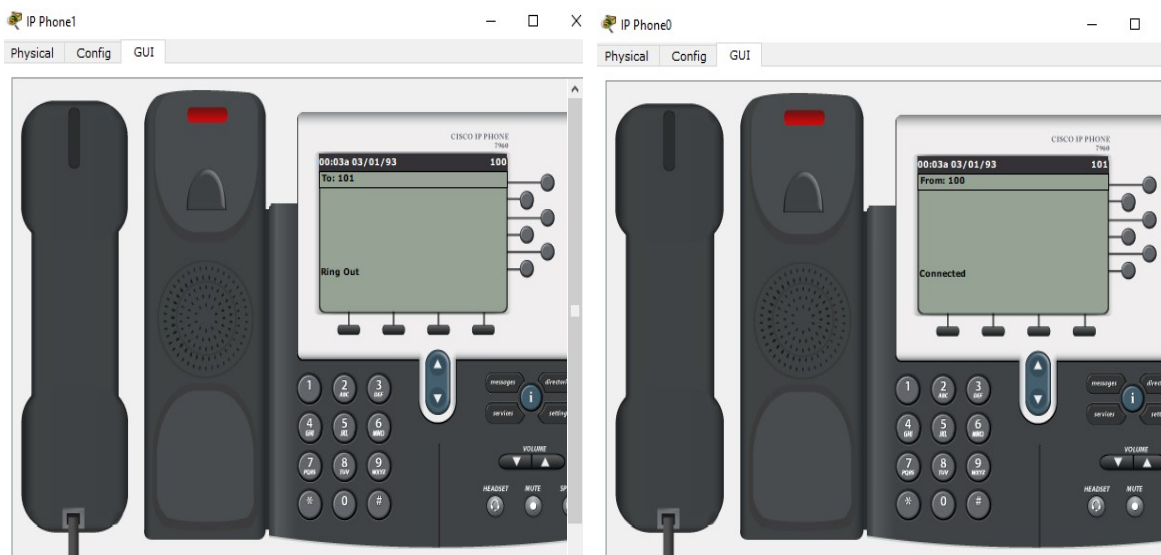
Router(config-ephone-dn)#num 101
```

- Configure a voice vlan on Switch:

```
Switch(config)#int fa0/8
Switch(config-if)#switchport voice vlan 1
Switch(config-if)#int fa0/9
Switch(config-if)#switchport voice vlan 1
```

Step 4:

Now, configure the phone directory from IPphone0 to IPphone1.



TELECOMMUNICATION NETWORK (TELNET)

Telnet (Telecommunication Network) is a network protocol used for remote access and management of networking devices over a network. It allows a user to log into a remote device (such as a router, switch, server, or computer) and interact with its command-line interface (CLI) as if they were physically connected to it. It establishes a basic, unencrypted, and insecure connection between the local and remote devices. When a user initiates a TELNET session, the login credentials and all data transmitted, including passwords and commands, are sent in clear text. Here are the key points about Telnet:

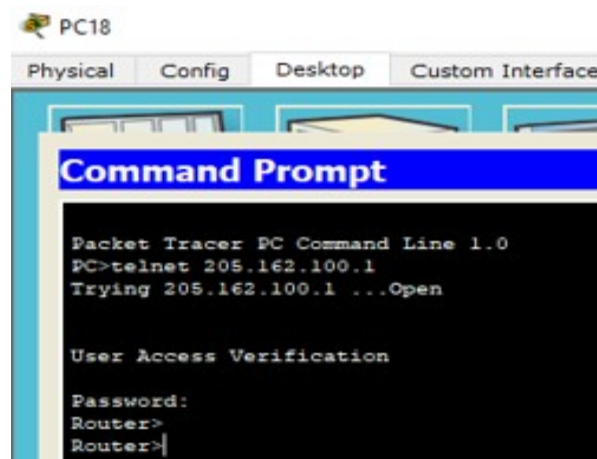
- **Protocol:** Telnet operates on the Application Layer of the OSI model. It uses the Transmission Control Protocol (TCP) to establish a reliable connection between the local and remote devices.
- **Port Number:** Telnet typically uses port number 23 for communication.
- **Plain Text Communication:** Telnet transmits data in plain text, meaning all the commands and responses are sent in clear text format. This lack of encryption poses security risks, as sensitive information, including usernames and passwords, can be intercepted by attackers.
- **Remote Access:** Telnet enables network administrators to remotely access and manage devices over the network, even if they are physically located at a different location.
- **Command-Line Interface (CLI):** Once a Telnet connection is established with a remote device, the user can access its command-line interface (CLI) and execute commands, configure settings, and perform various administrative tasks.

In Cisco Packet Tracer, you can use Telnet to remotely access and manage networking devices such as routers and switches. Here's a step to use Telnet in Cisco Packet Tracer.

- Double-click the router or switch you want to access via Telnet to open its configuration window.
- Go to the CLI tab to access the command-line interface of the device.
- Enter the following commands to enable Telnet:


```
Router(config)#line vty 0 15
Router(config-line)#password abc
Router(config-line)#login
Router(config-line)#enable password 123
```

- Save the configurations on the router or switch.
- Test Telnet access:
 - Go to the PC or laptop from which you want to access the router or switch via Telnet.
 - Open the command prompt or terminal on the PC.
 - Type the following command to initiate the Telnet connection:



- Once connected via Telnet, you can access the command-line interface (CLI) of the router or switch. You can then configure and manage the device remotely as if you were physically connected to it.

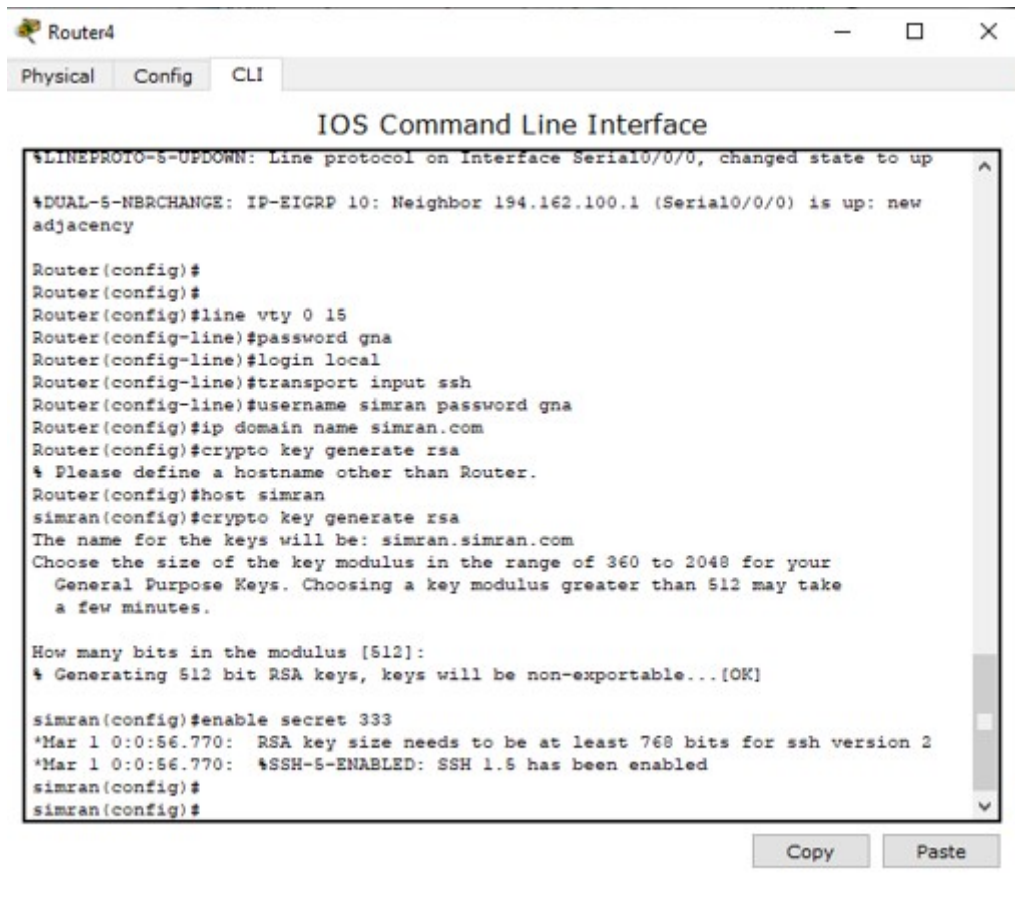
SECURE SHELL (SSH)

SSH (Secure Shell) is a network protocol that provides secure encrypted communication and remote access to networking devices and other systems. It is widely used for secure remote administration, file transfers, and other network-related tasks. SSH is considered a more secure alternative to protocols like Telnet, as it encrypts data during transmission, making it less vulnerable to eavesdropping and other security threats.

- **Protocol:** SSH operates on the Application Layer of the OSI model. It uses the TCP (Transmission Control Protocol) to establish a secure and reliable connection between the local and remote devices. . Here are the key points about SSH:
- **Port Number:** SSH typically uses port number 22 for communication.
- **Encryption:** One of the primary advantages of SSH is its ability to encrypt data during transmission, ensuring that sensitive information, including usernames, passwords, and command data, is secure and protected from unauthorized access.
- **Public Key Infrastructure:** SSH uses a public-key cryptography system for authentication. The user generates a public-private key pair, where the private key is stored securely on the user's local machine, and the public key is placed on the remote server. This allows for passwordless, yet secure, authentication.
- **Remote Access:** SSH enables network administrators to remotely access and manage devices over the network, just like Telnet. However, due to its encryption, it provides a higher level of security compared to Telnet.
- **Secure File Transfer:** SSH also supports secure file transfer protocols, such as SCP (Secure Copy) and SFTP (Secure File Transfer Protocol), allowing users to securely transfer files between devices.

The steps for SSH in cisco packet are given below:

- Double-click the router or switch you want to access via SSH to open its configuration window.
- Go to the CLI tab to access the command-line interface of the device.
- Enter the following commands to enable SSH:



The screenshot shows the CLI of Router4. The tabs at the top are Physical, Config, and CLI. The main window is titled "IOS Command Line Interface". The command history shows the following commands and their outputs:

```

$LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 194.162.100.1 (Serial0/0/0) is up: new adjacency

Router(config)#
Router(config)#
Router(config)#line vty 0 15
Router(config-line)#password gna
Router(config-line)#login local
Router(config-line)#transport input ssh
Router(config-line)#username simran password gna
Router(config)#ip domain name simran.com
Router(config)#crypto key generate rsa
% Please define a hostname other than Router.
Router(config)#host simran
simran(config)#crypto key generate rsa
The name for the keys will be: simran.simran.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

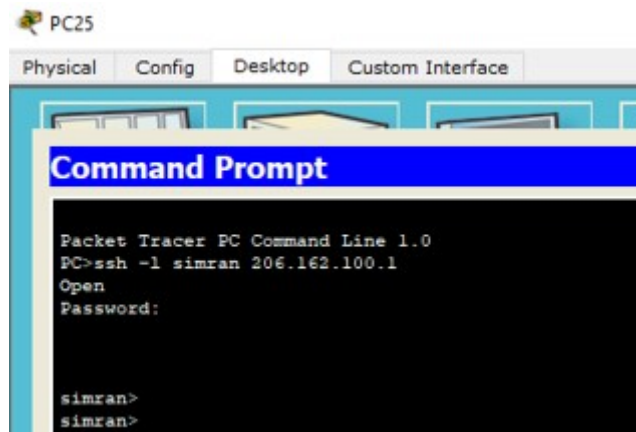
simran(config)#enable secret 333
*Mar 1 0:0:56.770: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:0:56.770: %SSH-5-ENABLED: SSH 1.5 has been enabled
simran(config)#
simran(config)#

```

At the bottom of the window, there are "Copy" and "Paste" buttons.

We need to change the default router name to generate rsa key.

At the last step of Configuring SSH, we can try to connect via SSH from PC to the router. To do this, we will open the command line on the PC and connect to the router with the below command.



The screenshot shows the Desktop of PC25. A "Command Prompt" window is open, displaying the following text:

```

Packet Tracer PC Command Line 1.0
PC>ssh -l simran 206.162.100.1
Open
Password:

simran>
simran>

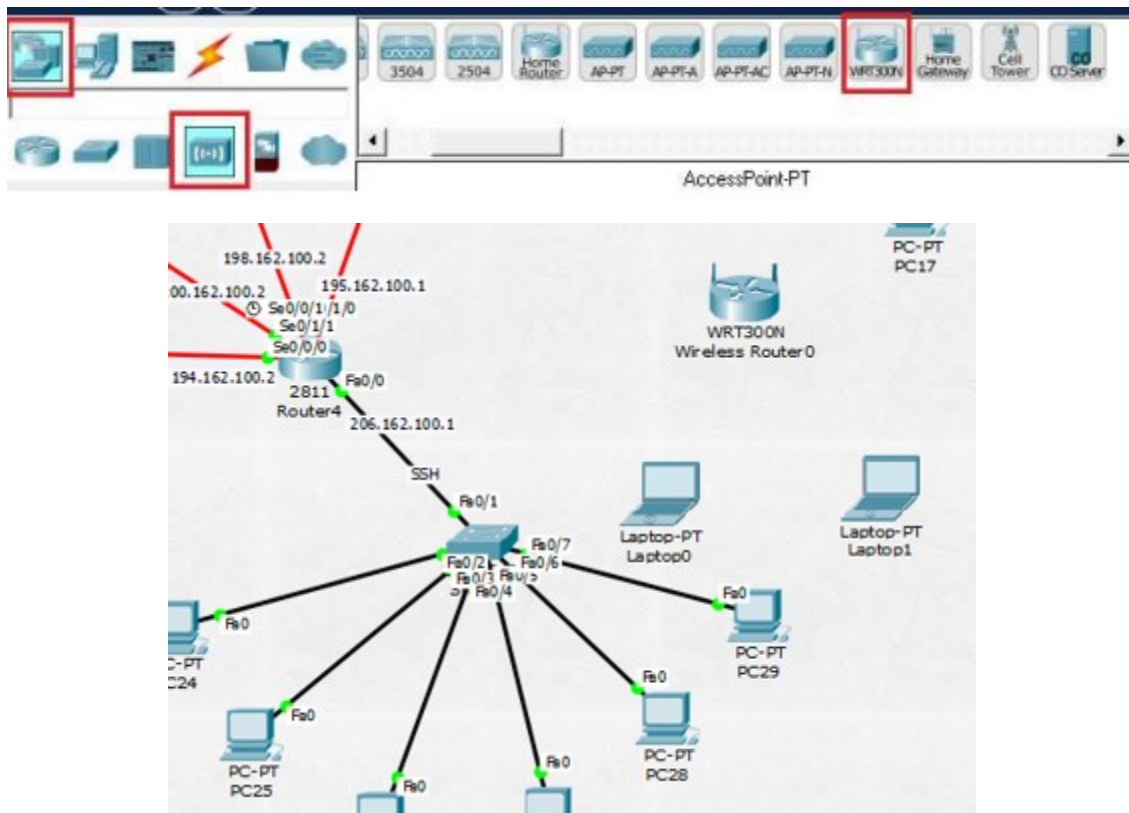
```

WIFI SERVER

The central device that provides wireless connectivity to Wi-Fi-enabled devices is typically referred to as a "Wireless Access Point" (AP) or "Wi-Fi Access Point." The AP acts as a bridge between the wired network and the wireless network, allowing devices such as laptops, smartphones, and tablets to connect to the network wirelessly. The Access Point broadcasts the Wi-Fi signal and provides a wireless connection to clients within its range. It serves as a gateway for Wi-Fi-enabled devices to access network resources and the internet.

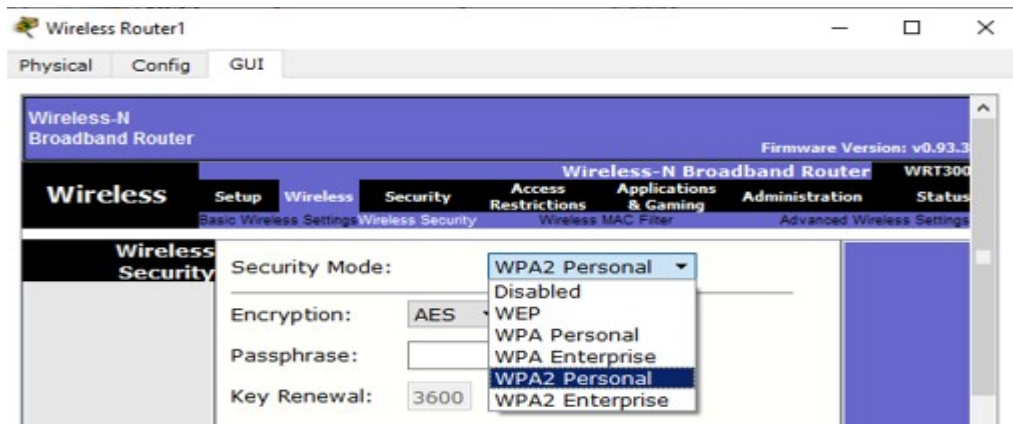
The steps for WiFi server in cisco packet tracer:

- There are varieties of wireless devices given in the packet tracer so we will select the wireless router WRT300N from the list and two laptop's:

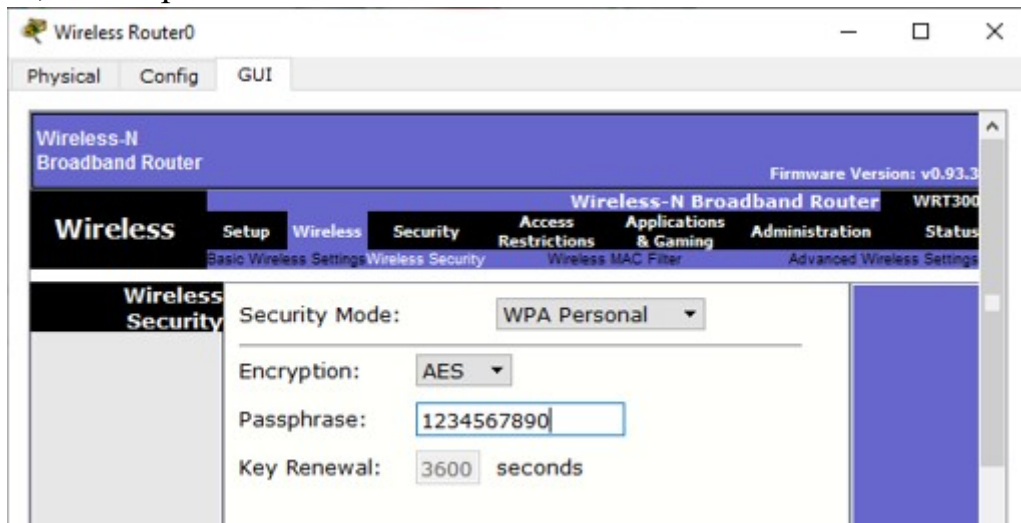


Now, we have to configure the wireless router. Most of the settings are already configured on the wireless router required to establish a wireless network however, we can change the configuration as per our requirement.

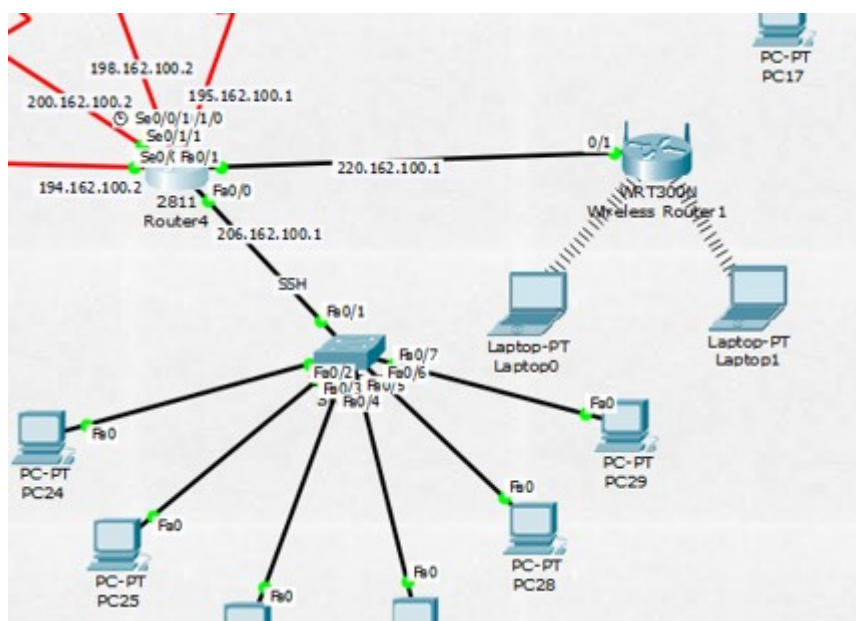
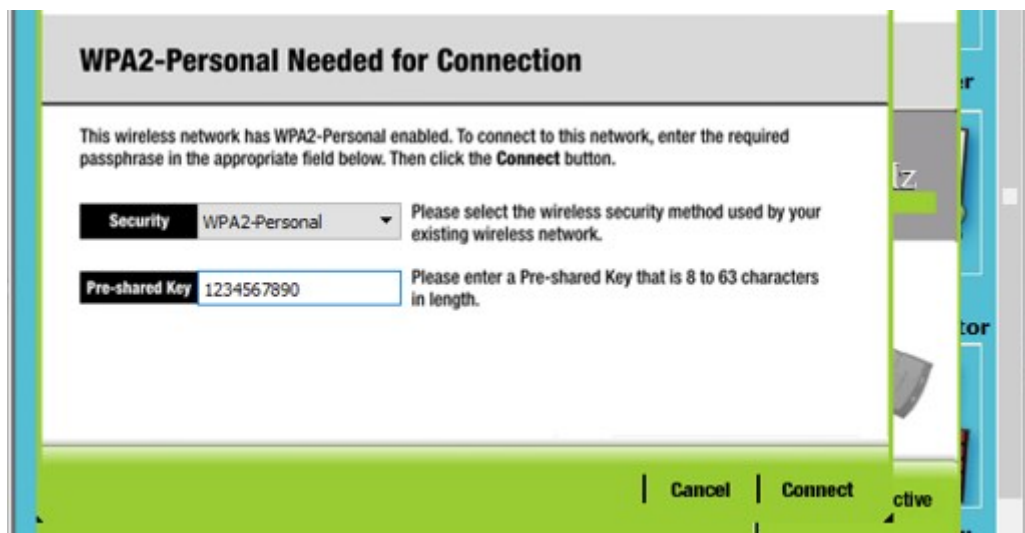
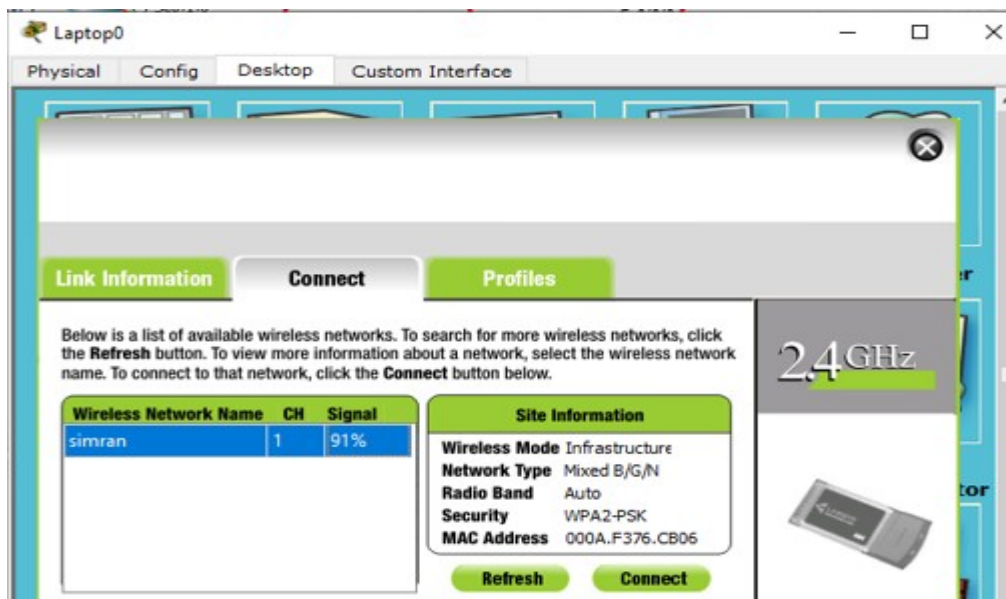
- Click on wireless and selects WPA2 Personal.



- Then, set the password and default name of wifi.



- Now connect wifi in laptop and put the password the wifi will connected to laptop.



SUBNETTING

- Subnetting is a technique used in computer networking to divide a larger IP network into smaller subnetworks called subnets.
- It involves creating a subnet mask that determines the network portion and host portion of an IP address.
- The subnet mask is a 32-bit value represented in the dot-decimal format, such as 255.255.255.0.
- Subnetting allows for efficient utilization of IP addresses by dividing them into smaller address ranges for different subnets.
- It improves network performance by reducing the size of broadcast domains and limiting network traffic within each subnet.
- Subnetting enhances network security by isolating traffic within subnets and allowing for the implementation of subnet-based access controls.
- The process of subnetting involves determining the number of required subnets based on network requirements.

Subnetting allows for better organization, efficient address allocation, improved network performance, and enhanced network security within computer networks. It is an essential technique for managing and optimizing IP networks.

Here's a simplified flowchart outlining the steps involved in subnetting in a computer network:

- Start
- Determine the number of required subnets
- Choose an appropriate subnet mask
- Calculate the number of subnet bits needed
- Calculate the remaining host bits
- Create the subnet address range
- Assign IP addresses to devices within each subnet
- End

▪ CALCULATION FOR SUBNETTING

FORMULA: $2^n - 1 \geq n$

Example: 194.162.1.1/30

➤ Calculate host bit:

$$2^n - 1 \geq \text{requirement}(30)$$

$$2^5 = 30$$

$$n = 5$$

➤ Calculate subnet mask:

According to this IP, subnet mask is 255.255.255.0

But host bit is 5

➤ On rearranging 11111000 =

$$(1*128)+(1*64)+(1*32)+(1*16)+(1*8)+(0*4)+(0*2)+(0*1)$$

$$=128+64+32+16+8$$

$$= 248$$

Now, subnet mask is 255.255.255.248

Here, $256 - 248 = 8$

Put the difference of 8 in each network.

194.162.1.1 .. 194.162.1.9 .. 194.162.1.17 .. 194.162.1.25 .. 194.162.1.33

➤ First address of each subnet is network id = 1,9,17.....

➤ Last address of each subnet is broadcast id = 8,16,24.....

➤ Network and broadcast id cannot be assigned to any device.

Now, all previous operations should be done for new IP, subnet mask and also routing protocol.

SUBNETTING NETWORK

