Practical File Of

Introduction to Computer Networks

CS156

Submitted By:

Garvit Arora

2110992205

G-23(B)

Submitted To:

Dr. Veeramanickam

Department of Computer Science & Engineering

Chitkara University Institute of Engineering & Technology, Rajpura, Punjab.

Index

EXPERIMENT NO. 1

Aim: Introduction of Cables, Network devices: Hub, Switches, Router, etc.

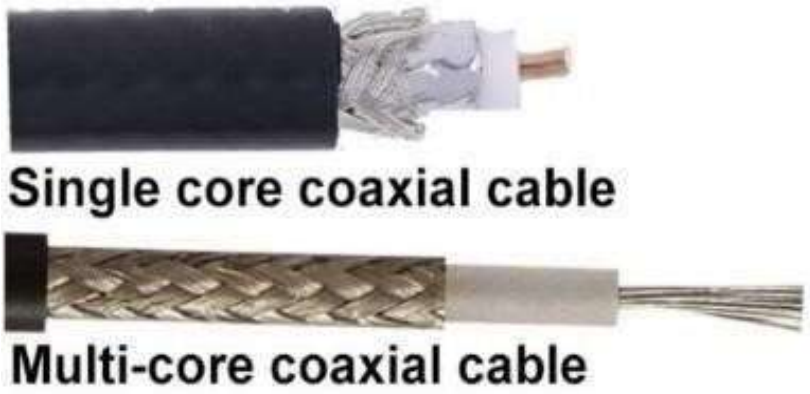
Material Required:

Coaxial Cables, Twisted Pair Cables, Fibre Optics cables, Switch, Hub, Router.

Theory:

Cables-

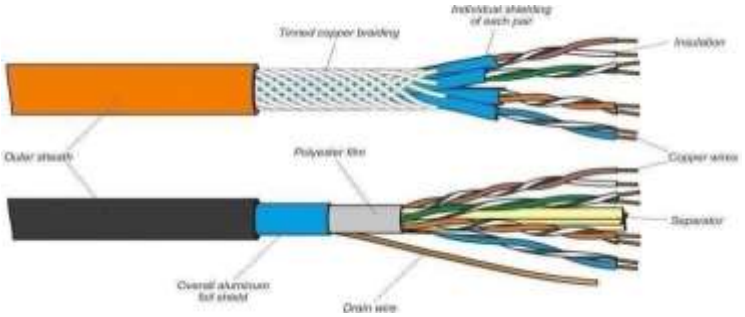
1) Coaxial Cables:



An electrical cable referred to as coax, has a copper conductor and an insulator shielding, along with a braided metal mesh that blocks signal interference and cross-talk. This cable is commonly called a coaxial cable.

The central copper conductor is employed for transmitting signals, with the insulator serving to insulate it. The insulator is then surrounded by a braided metal conductor that minimizes interference and cross-talk in electrical signals. A plastic layer of protection is added to the entire assembly to enhance its safety.

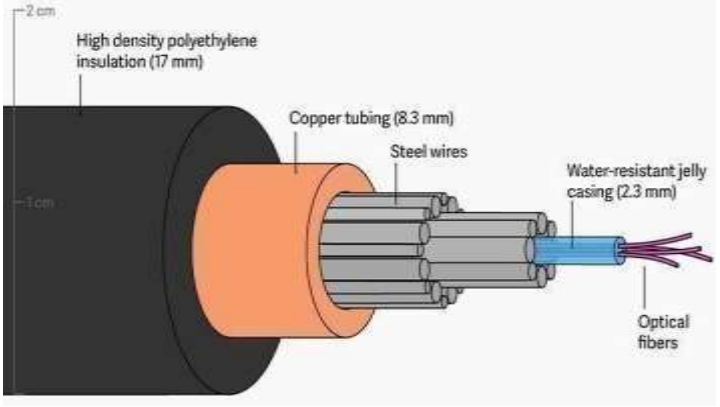
2) Twisted Pair Cable:



These cables are known as guided media and were invented by Alexander Graham Bell. Twisted pair cables consist of two copper conductors, each with insulation, that are twisted together.

One conductor carries the signal while the other is only used as a reference. The receiver determines the signal by the difference between the two conductors. The twisting reduces crosstalk and noise compared to parallel conductors. The number of twists per unit length determines the signal quality of the twisted pair cable.

3) Fiber Optic Cables:



A fiber optic cable uses glass or plastic to transmit signals as light. The structure of the cable features a glass core surrounded by a cladding that reflects light into the core and protected by a plastic jacket.

Data is transmitted via semiconductor lasers in the form of light along the thin glass or plastic fibers at 186,000 miles per second with minimal loss of intensity over long distances. The system is comprised of fiber optic cables made of delicate threads of glass or plastic.

Network Devices-

1) Hubs:

A hub is a device that acts as a multi-port repeater. It joins multiple wires from different branches, like the connector in star topology connecting different stations.
Hubs are unable to sort data, so data packets are sent to all connected devices. This means the collision domain for all hosts connected via the hub remains one. Additionally, hubs lack the ability to determine the optimal path for data packets, resulting in inefficiencies and waste.

2) Switch:

A switch is a network component that links other devices to Ethernet networks via twisted pair cables. It employs packetswitching technology to receive, store, and forward network data packets.

The switch has a database of network addresses for all connected devices. Upon receipt of a packet, it examines the destination address and forwards the packet to the appropriate port. The packet is first verified for network errors, such as collisions, prior to forwarding. The switch operates in full-duplex mode for data transmission. Its data transfer rate can be double that of other network devices, like hubs, resulting in improved network speed even during heavy traffic.Using multiple switches further boosts data transmission speed on a network.

4) Router:

A router is a device, similar to a switch, that forwards data packets based on their IP addresses. It operates at the Network Layer and is designed to interconnect LANs and WANs. It holds a routing table that dynamically updates to help it determine the best path for data packet routing. Routers break up the broadcast domains of devices connected through them. There are various types of routers, but many of them provide a bridge between LANs (Local Area Networks) and WANs (Wide Area Networks).

A LAN is a group of interconnected devices located in a specific geographical area and often needs just one router. A WAN, on the other hand, is a vast network spread over a wide area and necessitates multiple routers and switches to function effectively, especially for organizations and companies operating in multiple locations.

EXPERIMENT NO. 2

Aim: Installation and introduction to packet tracer.

Material Required:

Good internet connection, login credentials to netacad.com.

Theory:

-> Packet Tracer is a network simulation tool created by Cisco that provides a visual interface for users to design network setups and simulate the behavior of modern computer networks.

The software allows for the simulation of Cisco router and switch configurations through a simulated command line.

Its main objective is to give students practical experience in networking and help them gain skills in Cisco technology. It should be noted that since the protocols are only implemented through software, the tool can not replace physical routers or switches.

Additionally, the tool encompasses not only Cisco products but also a wide range of networking devices.

Procedure:

1) Login to netacad.com

2) Scroll down and select the card where the packet tracer is written.

3) Scroll down and then select your operating system and then click on download.

4) After successful installation, the initial screen would be as shown in the figure.

EXPERIMENT NO. 3

Aim:

Simulation of Network Devices (HUB, Switches, routers) and connecting more than two computers using Switch to Topologies like Star, Mesh, Ring, Bus, and Hybrid.

Material Required:

Cisco Packet Tracer Tool.

Theory:

1. Hub:-

An Ethernet hub, active hub, network hub, repeater hub, multiport repeater, or simply hub is a network hardware device for connecting multiple Ethernet devices together and making them act as a single network segment.

2. Switches:-

These are electronic components that can disconnect or connect the conducting path in an electrical circuit, interrupting the electric current or diverting it from one conductor to another. **3. Routers:-**

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions between networks and on the global Internet. Data sent through a network, such as a web page or email, is in the form of data packets.

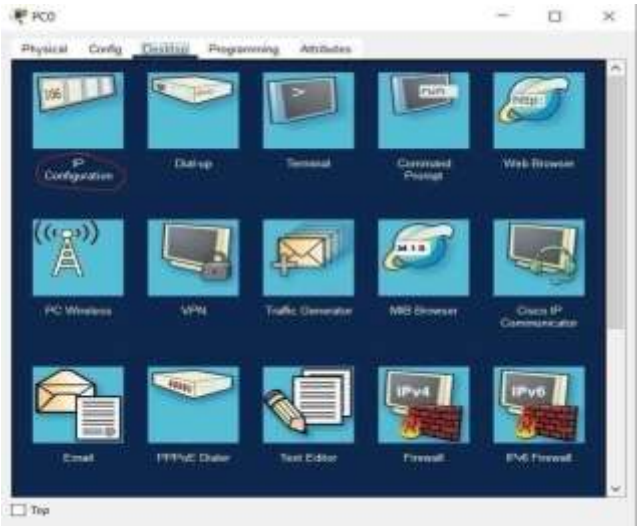
Procedure:

- Step1.

  We will select 4 devices and a switch as shown in the figure below.

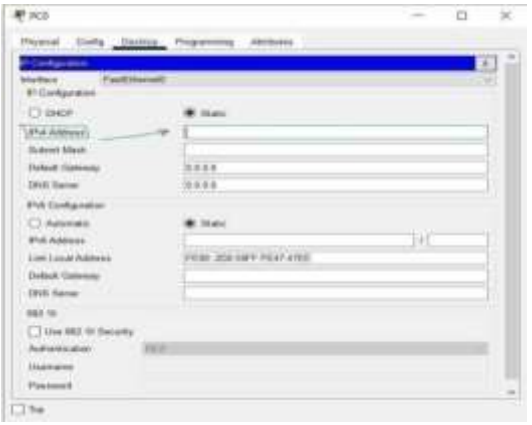
- Step 2.

  Now, we need to give an IP address to the device by clicking on the device and selecting desktop from the top and then choosing the IP configuration option.



- Step 3.

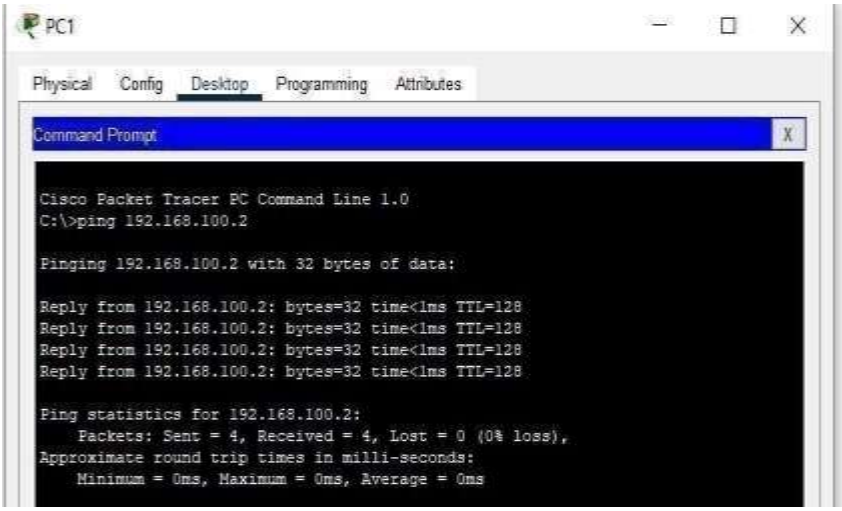
  Now, we need to provide an IP address for our devices.

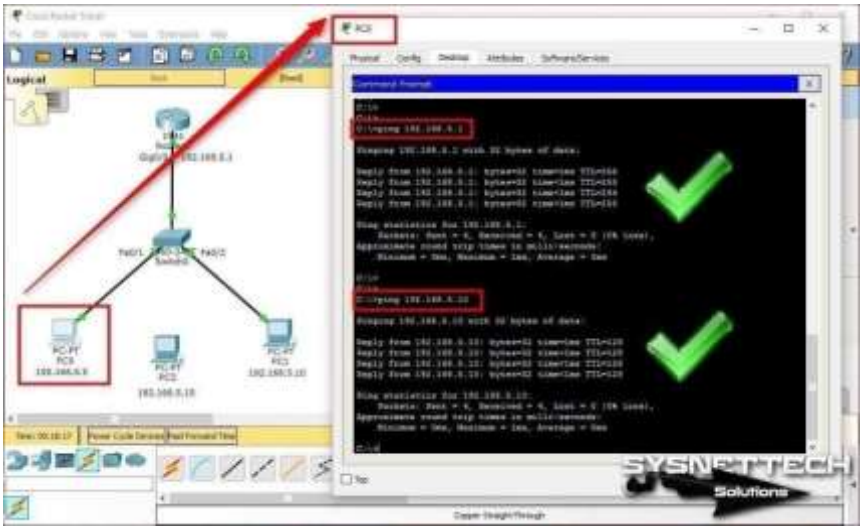


- Step 4.

  Now, we will run the ping command to check whether the reply is coming from the target device or not, and if the reply successfully comes then it means all connections are properly connected.

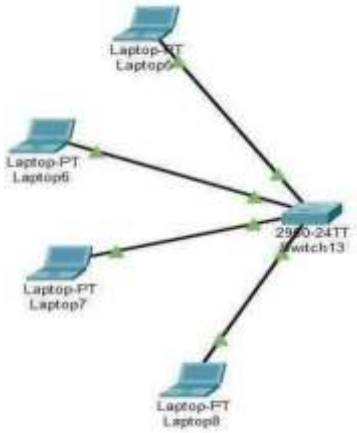
  The syntax for the ping command:- **ping <ip address_target>**





Result:-

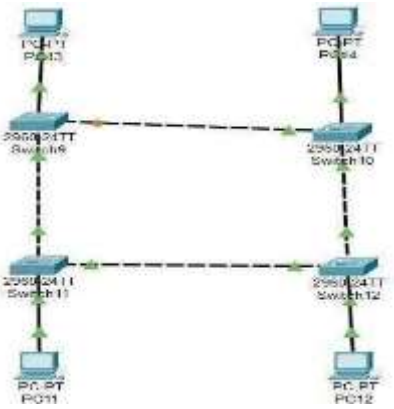
- **Star Topology:-**



Star topology is a network topology in which each network component is physically connected to a central node such as a router, hub, or switch. In a star topology, the central hub acts like a server and the connecting nodes act like clients. When the central node receives a packet from a connecting

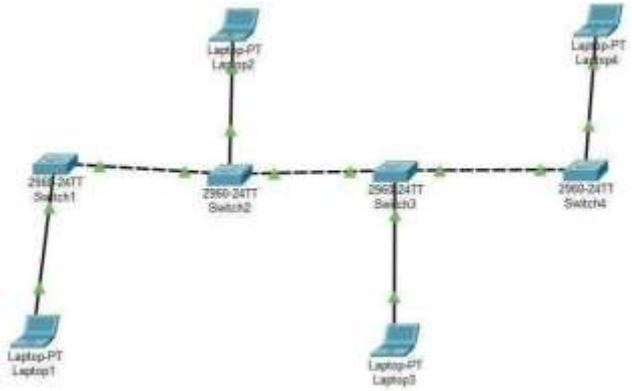
node, it can pass the packet on to other nodes in the network. A star topology is also known as a star network.

- **Ring Topology:-**



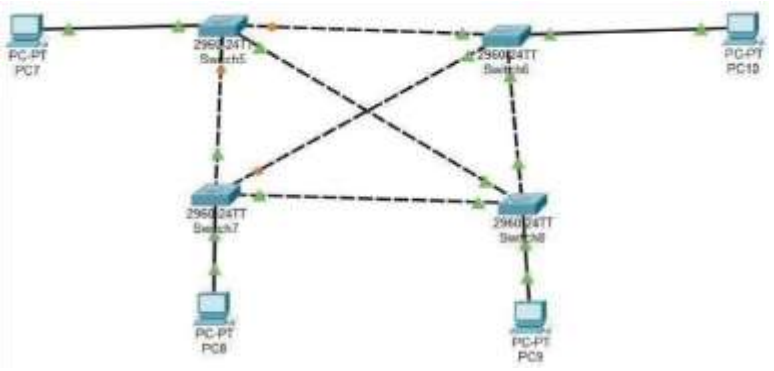
Ring topology is a type of network topology in which each device is connected to two other devices on either side via an RJ-45 cable or coaxial cable. Data is commonly transferred in one direction along the ring, known as a unidirectional ring. The data is forwarded from one device to the next until it reaches the intended destination. In a bidirectional ring, data can travel in either direction.

- **Bus Topology:-**



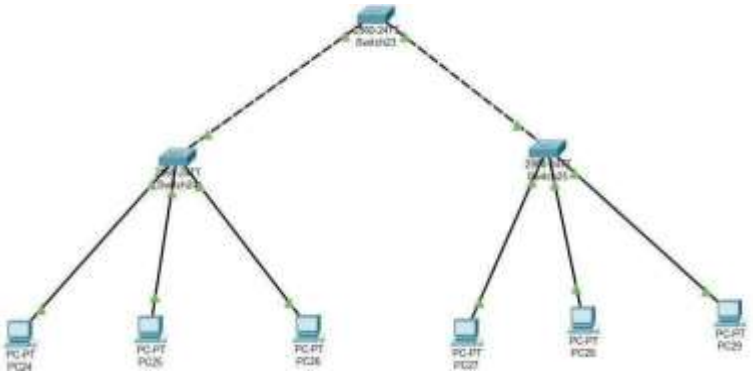
Alternatively called line topology, bus topology is a network setup where each computer and network device is connected to a single cable or backbone. Depending on the type of computer network card, a coaxial cable or an RJ-45 network cable is used to connect them.

- **Mesh Topology:-**



A mesh topology is a network setup where each computer and network device is interconnected with one another. This topology setup allows for most transmissions to be distributed even if one of the connections goes down. It is a topology commonly used for wireless networks. Below is a visual example of a simple computer setup on a network using a mesh topology.

- **Tree Topology:-**



Tree topology is a sort of structure in which each node is related to the others in a hierarchy. In a topological hierarchy, there are at least three distinct levels. Sometimes it is also called hierarchical topology as in this topology, all elements are arranged like the branches of a tree. It is a lot like the star and bus topologies.

We Simulated Network Devices (HUB, Switches, routers) Successfully connecting more than two computers using Topologies like Star, Mesh, Ring, Bus, and Hybrid.

EXPERIMENT NO. 4

Aim:

Basic commands of Routers: hostname, password, Show Run, Show IP int brief, Assigning IP addresses to interfaces .

Cisco Router basic commands:

1) Host name

To specify or modify the host name for the network server, use the hostname global configuration command. The host name is used in prompts and default configuration filenames. The **setup** command facility also prompts for a host name at startup.

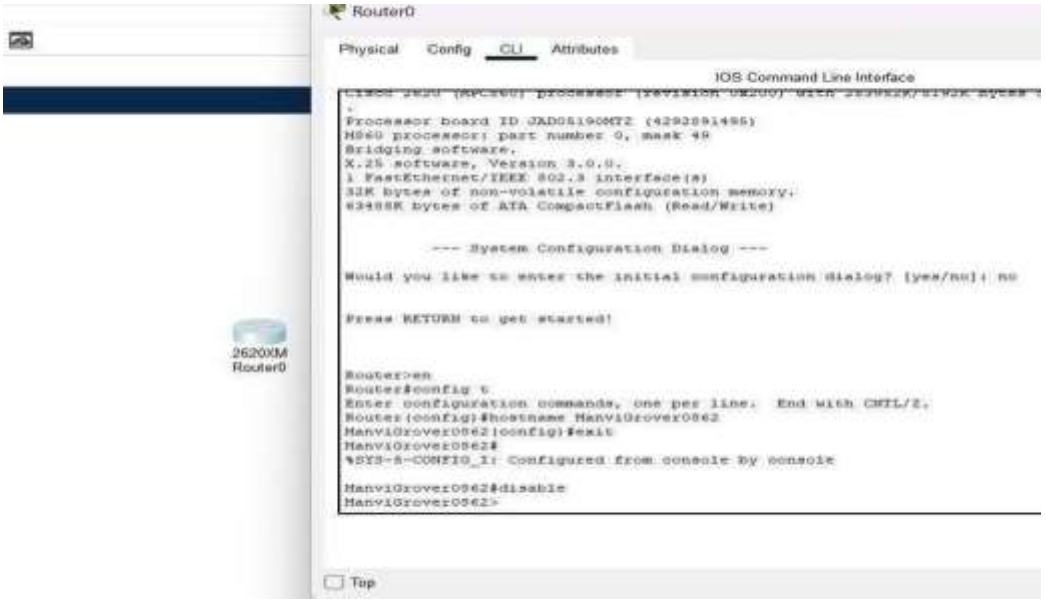
hostname *name*

Syntax Description

name	New host name for the network server.

Defaults

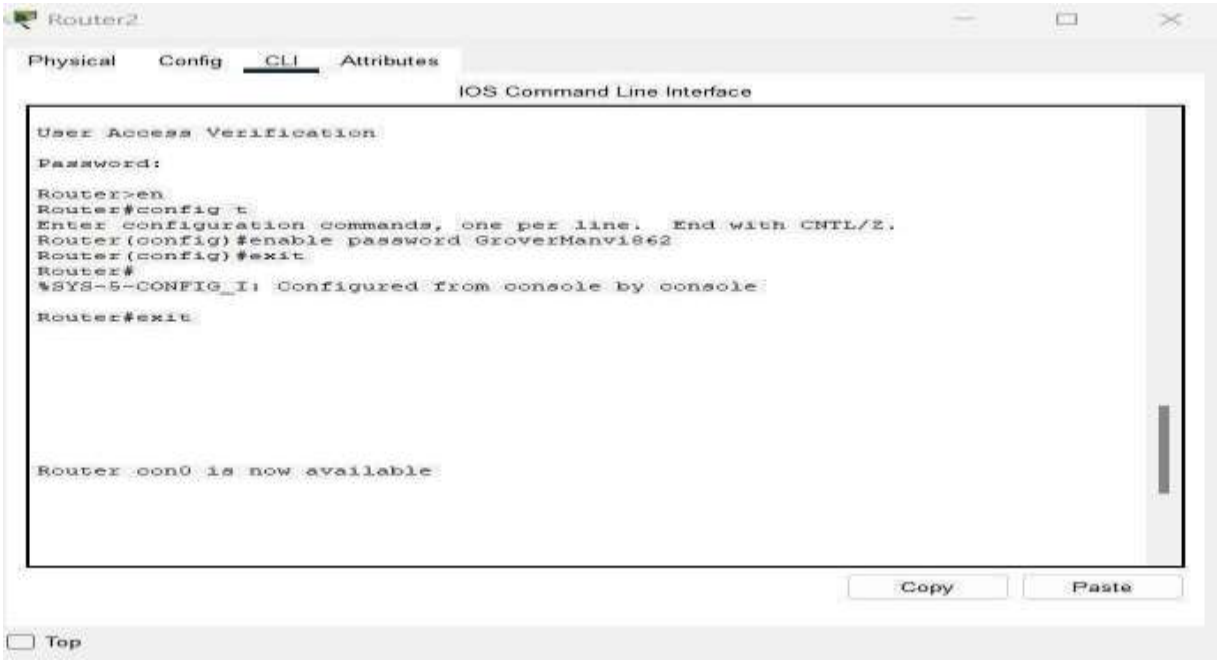
The factory-assigned default host name



2) Password:

1. **Enablepassword :** The enable password is used for securing privilege mode. This These are replaced by secret passwords nowadays.

router(config)#enable password GroverManvi862



2. **Enable Secret password :** This is also used for securing privilege mode but the d the difference is that it will be displayed as a cipher in “show

runningconfiguration". This password will override the enable password if both passwords are set.

router(config)#enable secret **GroverManvi0862**

2) Show Run:

Type **"show run"** or **"show start"** to show the applicable config. The config will display without any breaks or pauses.

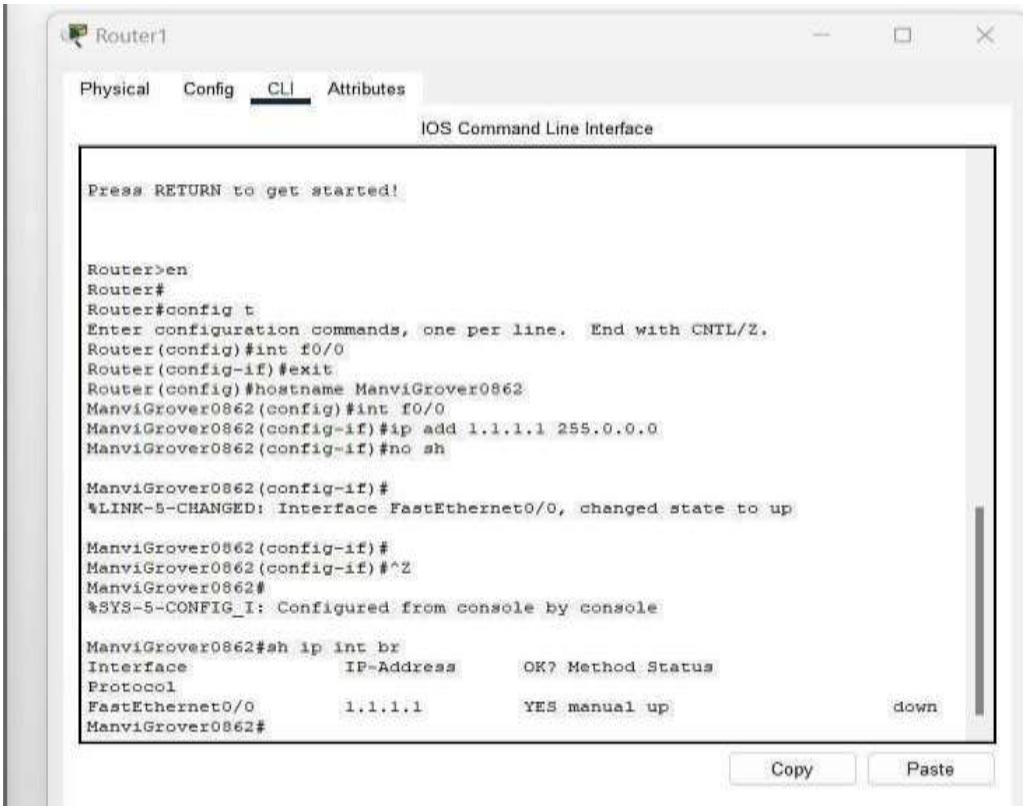
3) show ip:

To display IP configuration data, enter the show ip command in User Exec mode or Privileged Exec mode.

❾**show ip [address-table | route | http [server secure]] Syntax Description**

Address table	(Optional) This keyword displays the address information of Ethernet interface ports, Ethernet interface cards, and InfiniBand interface cards. It lists the IP addresses, netmasks, broadcast formats, reassembly sizes, and whether or not the IP address is a primary or backup.

	(Optional) This keyword displays the Classless Inter-Domain Routing (CIDR) forwarding records or routes (both static and dynamic) of all IP routes to system ports. Included in this information are the route destination, route type, route protocol, next hop, and port used.
http	(Optional) Displays current HTTP settings.
server secure	(Optional) Displays current secure HTTP server settings.



4) Assigning IP addresses to interfaces:

Assign an IP address to that interface with the 'ip address' command followed by the IP address and the subnet mask for that interface. Run the 'show IP interface brief' command again to verify the IP address has been assigned to the network interface.

EXPERIMENT NO. 5

AIM:

To do peer to peer connectivity , assign the IP addresses and share the resources.

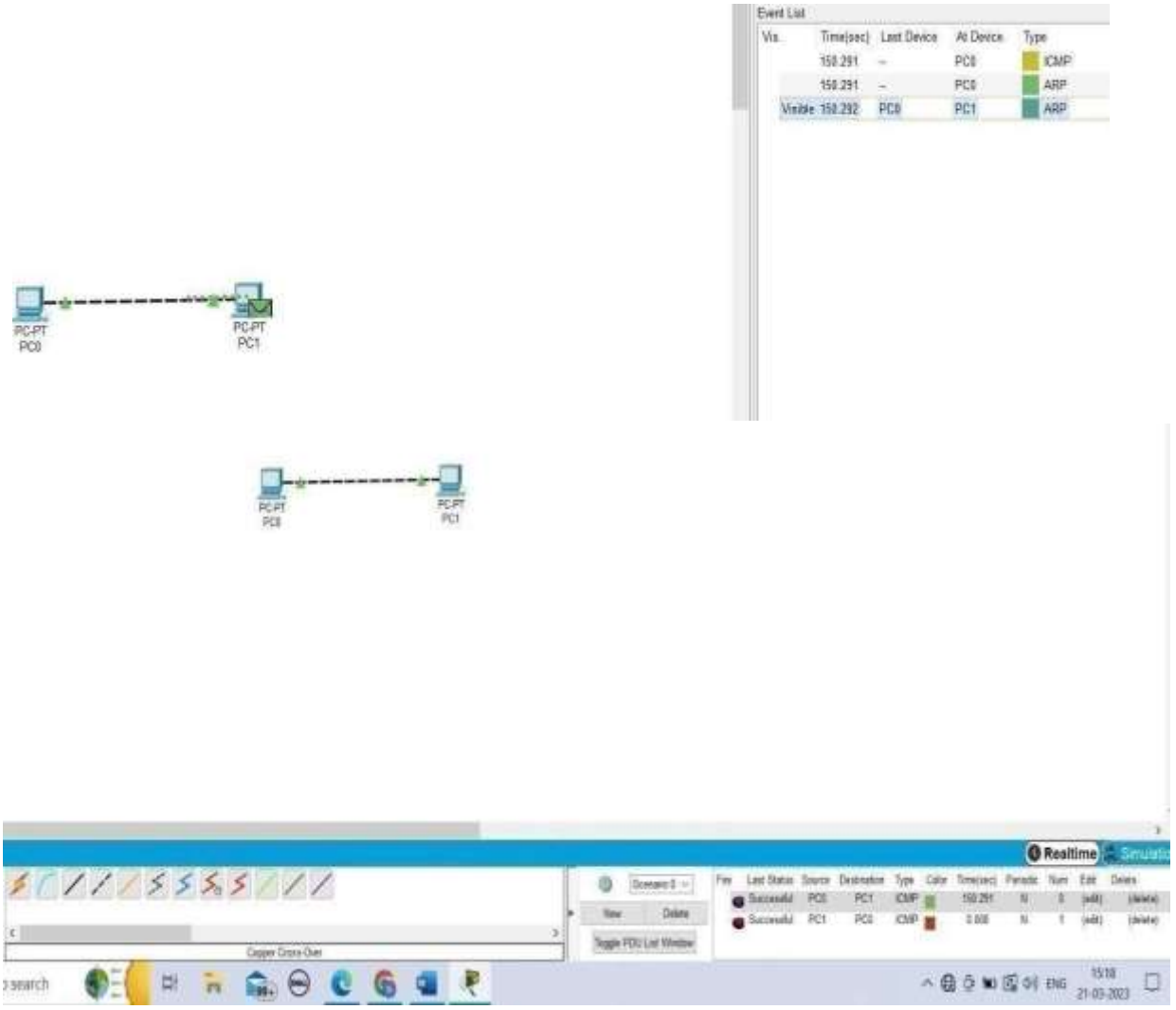
Peer to Peer Network :- In peer to peer network there is no center server in the network. In this each computer is connected to each other and act as a node. This network came into existence in 1970's. Each node is working independently so the network to stop working, all the nodes need to stop working individually.

Types of peer to peer network:-

1: Structured p2p network:- This network is designed using software usually it is not easy to set up but it gives easy access to users to find the content.

2: Unstructured p2p network:- In this devices are connected randomly to each other and because of this users find difficulty in finding the content.

3: Hybrid p2p network:- This network is the combination of structure p2p network and unstructured p2p network.



In these pictures we do p2p connectivity give one pc ip address 10.0.0.1 and to the other one 10.0.0.2 and then send packets as we can see the packets have been sent to another pc successfully.

EXPERIMENT NO. 6

Aim:

Subnetting with Class A, B, C with different IP addresses.

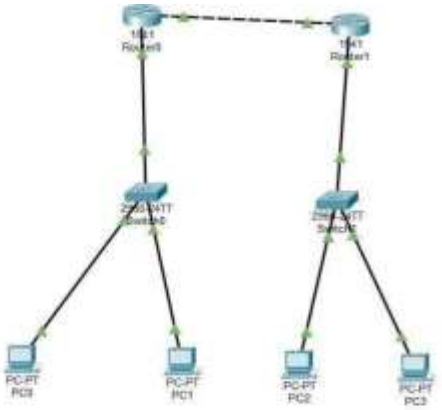
In this we use static routing. Whenever we divide a large IP network into small IP networks that is called subnetting. There are many benefits of subnetting it enhance network work. It allow you to control traffic flow in a better way. It improves network security by controlling the network flow and route may help you to identify the risk.

It provide regulation on network growth you can even calculate the size of network by using host formula.

An IP address is the combination of two addresses host address and Network address. In A class 8 bits are reserved for network address, In B class 16 bits are reserved for networkaddress and In C class 24 bits are reserved for network address. In all the three classes last two bits are for host address.

The IP address of class A is used for host address. When the first bit is zero in IP address it means it belongs to class A. This class has 8 bits for networking and 24 bits for subnet mask.

When the IP address contain 10 digits in starting it means it belongs to class B and are in the range of 128.0.0.0 to 192.255.255.255. This class has 16 bits for networking and 16 bits for subnet mask.



In this picture as we can see we do subnetting with class A , B and c and assign them different IP addresses.

EXPERIMENT NO. 7

AIM:

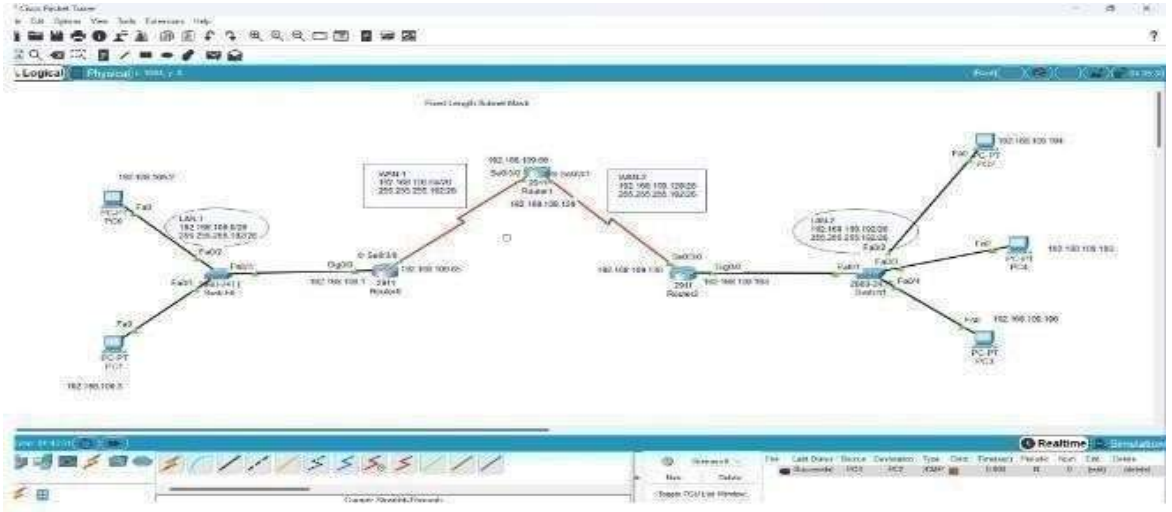
Subnetting of Class A, B and C using FLSM

FLSM: A fixed-length subnet mask (FLSM) is a type of enterprise or provider networking in which a block of IP addresses is divided into numerous subnets of equal length, i.e., an equal amount of IP addresses. Within a private network's subnets, FLSM streamlines packet routing.

Subnetting: Subnetting refers to the process of using a subnetting mask to divide a network into numerous smaller subnetworks. Every subnet in FLSM has the same amount of IP addresses. Another way to put it is that the same amount of IP addresses are allotted to each subnet. As a result, each network will use the same subnet mask.

The IP address of class A is used for host address. When the first bit is zero in IP address it means it belongs to class A. This class has 8 bits for networking and 24 bits for subnet mask.

When the IP address contain 10 digits in starting it means it belongs to class B and are in the range of 128.0.0.0 to 192.255.255.255. This class has 16 bits for networking and 16 bits for subnet mask.



EXPERIMENT NO. 8

AIM:

Subnetting of Class A, B, and C using VLSM.

Theory:

Variable length Subnet mask (VLSM) is a technique used in IP network design to create a subnet with different subnet masks.VLSM allows network administrators to allocate IP addresses more efficiently and effectively, by using smaller subnet masks for subnets with fewer hosts and larger subnet masks for subnets with more hosts.

VLSM allows network administrators to create subnets with different subnet mask to more effectively utilize IP addresses. Using the example VLSM could be used to assign a subnet mask of 255.255.255.128 to smaller subnet with 10 hosts. which would provide 126 available IP address and a subnet mask of 255.255.255.192 to the larger subnet with 50 hosts, which would provide 62 available Ip addresses.

Procedure–

In VLSM, subnets use block Suze based on requirement so subnetting is required multiple times. Suppose there is an administrator that has four departments to manage. These are sales and purchase department with 120 computers, development departments with 50 computers, accounts department with 26

computers and management department with 5 computers. If the administrator has IP192.168.1.0/24,department wise Ips can be allocated by following these steps:

1. For each segment select the block size that is greater than or equal to the actual requirement which is the sum of host addresses, broadcast addresses and network addresses.

2. Arrange all the segment in descending order based on the block size that is from highest to lowest requirement. **Advantages:**

1. In fixed length subnet mask subnetting (FLSM),all the subnets are of equal size and have equal number of hosts but in VLSM the size is variable and it can have variable number of hosts thus making the IP addressing more efficient by allowing a routed system of different mask length to suit requirements.

2. In FLSM there is a wastage of IP addresses but in VLSM thers is a minimum wastage of IP addresses.
3. FLSM is preferred For private IP addresses while for public Ip addresses VLSM is the best option.

Disadvantages :

Complexity: VLSM requires more advanced planning and configuration compared to traditional subnetting, which can increase the complexity of the network design and administration.

Compatibility issues: VLSM may not be compatible with older networking equipment or protocols, which can limit its usefulness in certain environments.

EXPERIMENT NO. 9

Aim:

To perform static routing, default routingby using 2 and 3 routers.

Static routing is a form of routing thatoccurs when a router uses a manually- configured routing entry, rather than information from dynamic routing traffic. In many cases, static routers are manually configured by a

network administrator by adding in entries into a routing table, though this may not always be the case.

In computer networking, the default route is a configuration of the Internet protocol (IP) that establishes a forwarding rule for packets when no specific address of a next-hop host is available from the routing table or other routing mechanisms.

We can say that defaultrouting can be considered a special type of static routing.

The defaultroute is used to send data packets to an unknown targetto a single next hop address.

In static routing routers are user defined.

Static routing is implemented in small networks. In static routing additional resources are not required.

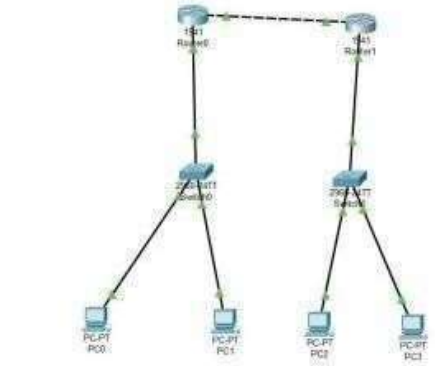
Static routing is difficult to configure. Static routing is non

adaptive. If static routing fails it will disrupt the rerouting. It is

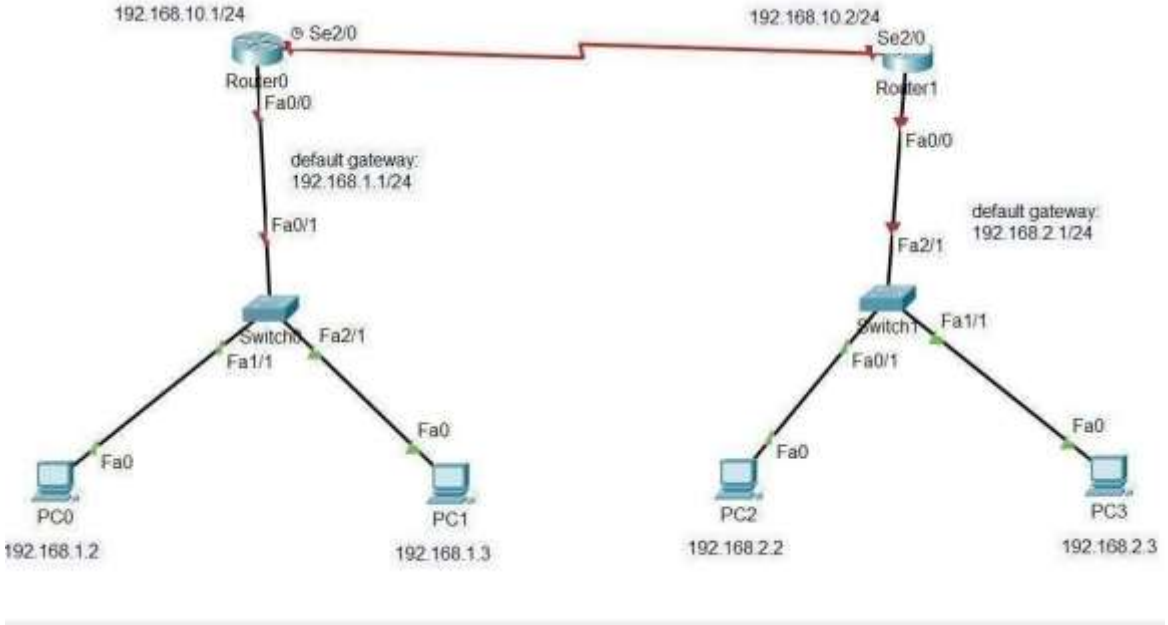
manual.

Default routes handle traffic for unknown destinations and all IP requests are sent to a single fixed gateway. Default routers are not fault tolerant. They are less resources and bandwidth intensive.

Static Routing



Default Routing



EXPERIMENT NO. 10

AIM:

To Perform Dynamic Routing using RIP (RIP-V1 and RIP-V2).

Routing is a process of finding a path and then sending packets across networks, the device which performs these functions is called a router. Types of Routing:

- **Static Routing**

- **Dynamic Routing**

Configuration of RIP Versions 1 and 2 :

Step 1: Open Cisco Packet Tracer (log in if not already done so).

Step 2: From the Network Devices category, select routers, and from the devices drag 4 2911 routers into the workspace (we can choose any Routers, but we're choosing 2911 for the number of ports available so that modules aren't required)

Step 3: Select the End Devices sub-category from End Devices, and drag 3 PCs into the workspace.

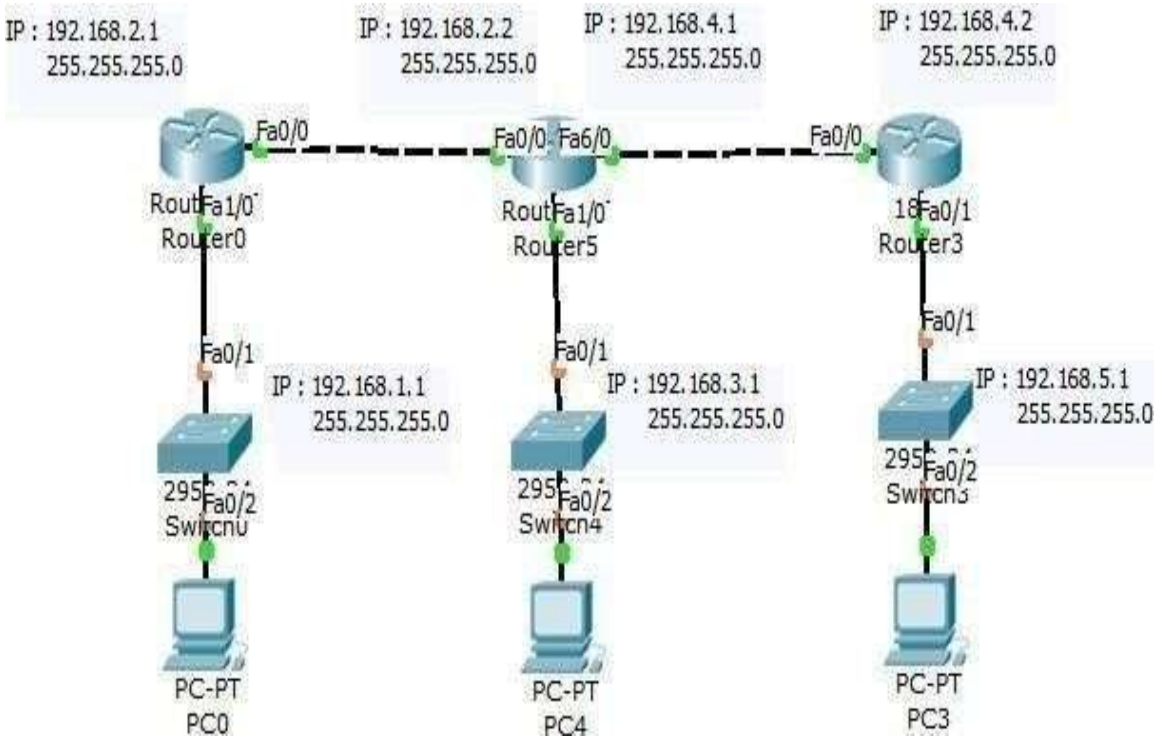
Step 4: Connect all the devices using crossover cables.

Step 5: Assign IP addresses to PCs and Router interfaces according to the topology in the above image.

- For configuring a PC, Click on a PC and a window will open, select desktop and then IP configuration, and enter the required IP, subnet mask, and default gateway. An image is shown below as an example for PC0. Step 6: Now for configuring routing, first click Router 0, navigate to the CLI tab, enter no for entering initial configuration mode if prompted, and then enter the following commands on the CLI prompt to configure RIP version 1.

Step 7: Similarly configure other routers, Router1,Router2, and Router3 according to connected networks using the above commands as a reference and using their specific neighbour network IPs in the above- mentioned syntax.

Step 8: Test the connection by using the ping utility in the command prompt in a PC to reach another PC in other networks, the first packet might possibly not reach as it takes time for config to apply. The output might be similar to the image shown below.




```
Router#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#
Router#
Router#
Router#
Router#conf
Router#configure ter
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#rou
Router(config)#router ri
Router(config)#router rip
```

EXPERIMENT NO. 11

AIM:

To Perform Dynamic Routing using EIGRP.

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing network-layer Protocol that works on protocol number 88. EIGRP supports classless routing, VLSM, route summarization, load balancing, and many other useful features. It is a Cisco proprietary protocol, so all routers in a network that is running EIGRP must be Cisco routers but now EIGRP is moving towards becoming an open standard protocol.

EIGRP exchanges messages for communication between the routers operating EIGRP.

By default, the network command uses a classful network as the parameter.

All interfaces inside that classful network will participate in the EIGRP process. To enable EIGRP only on specific interfaces, a wildcard mask can be used.

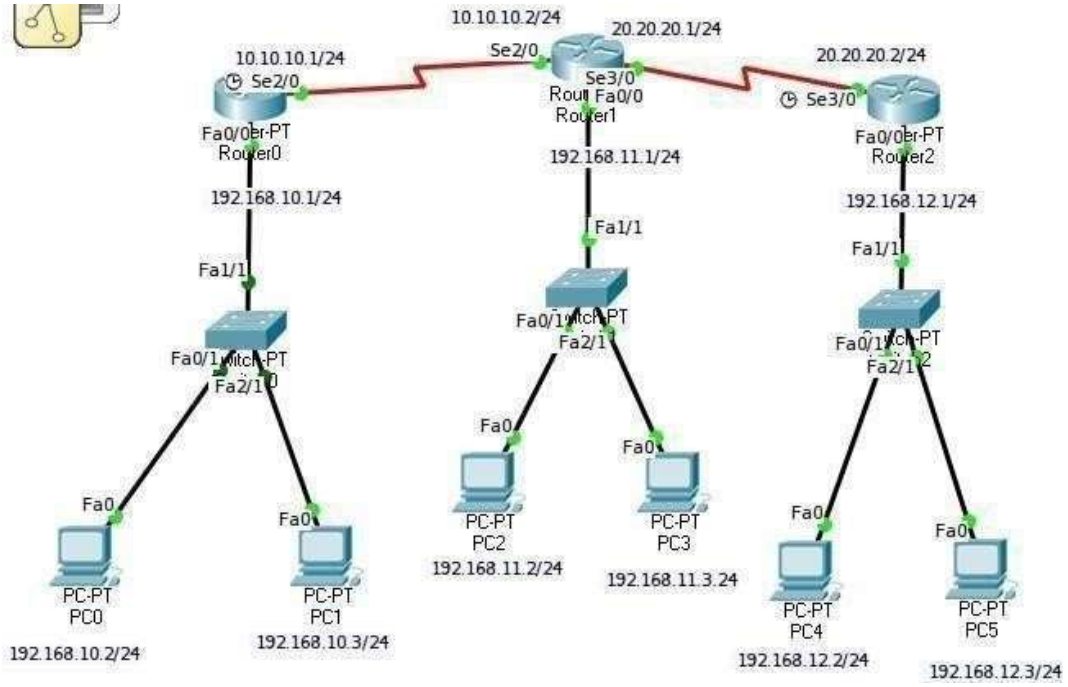
Troubleshooting – As configured EIGRP, user should see problems occurring in forming neighbourship between EIGRP operating routers. The neighbourship will not be formed if:

- The interface is configured as passive
- The k values don't match
- The autonomous system number is different
- EIGRP authentication is misconfigured
- Interface between devices is down

If in case, adjacency is up but the router doesn't receive the network updates then these can be the following reasons:

- Proper networks are not advertised
- ACL is applied on the interface

- Auto-summary command cause summarization of networks that are not needed.



EXPERIMENT NO. 12

Aim:

To perform Dynamic Routing using OSPF with single area concept and multiple area concept.

Theory:

OSPF as a link-state routing protocol identifies two parameters, the “link” representing the interface and the “state” representing the relationship of the interface to the neighbouring router. Compared to the traditional distance vector routing protocols such as EIGRP or RIP, OSPF has the following advantages:

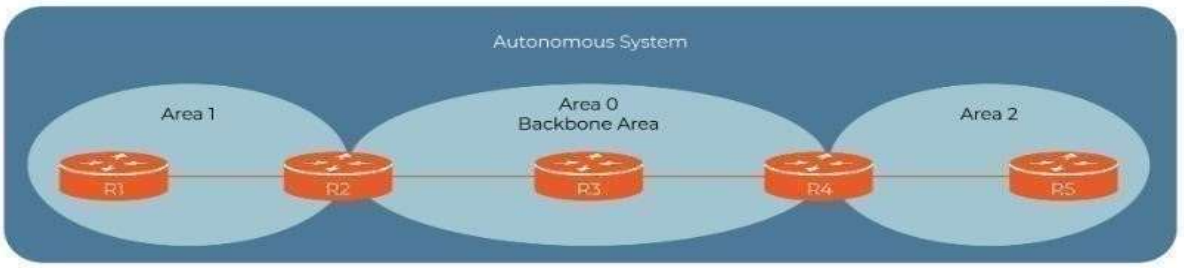
- More scalable approach.
- Efficient use of updates by sending trigger updates.
- Each router has a full map of the topology. Responds quickly to topology changes.

Also, OSPF relies on independent transport and not IP, has support for Variable Length Subnet Mask (VLSM) and authentication, and uses a simple approach for the calculation of the metric.

Hierarchical Structure of OSPF:

OSPF uses a two-layer network hierarchy, consisting of an Autonomous System (AS) that represents a collection of networks under a common administration that usually shares a common routing strategy, and an Area representing multiple grouped networks.

When implementing OSPF, Area 0 or the backbone area must be defined and is usually enough for normal operations in a network. However, in large enterprises, there is a need for a multi-area approach. In such a design, all additional areas must be directly connected to the backbone area, which limits the flexibility of OSPF.




```
Branch(config)#router ospf 1
Branch(config-router)#network 10.0.0.0 0.255.255.255.255 area 0
```

```
HQ(config)#router ospf 1
HQ(config-router)#network 172.16.1.0 0.0.0.255 area 0
HQ(config-router)#network 192.168.1.2 0.0.0.0 area 0
```

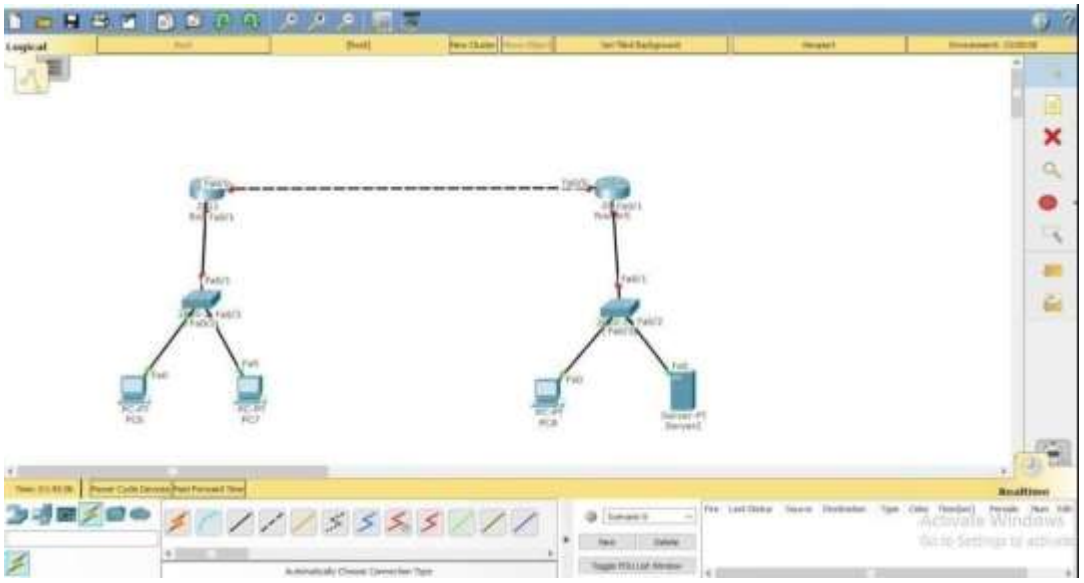
EXPERIMENT NO. 13

AIM:

To Create and Apply ACL: Standard and Extended Theory:

ACL - Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

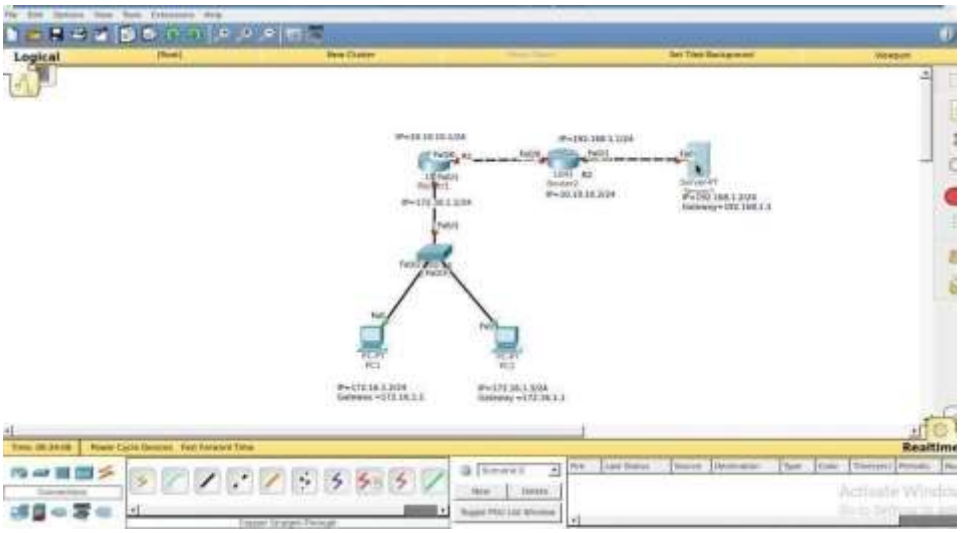
1. **Standard Access List** - These are the Access-list which are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300- 1999, the router will understand it as a standard ACL and the specified address as the source IPaddress.



R1(config)# ip access-list standard blockacl
R1(config-std-nacl)# deny 172.16.40.0 0.0.0.255
R1(config-std-nacl)# permit any
R1(config)# int fa0/1
R1(config-if)# ip access-group blockaclout

2. **Extended Access List** - It is one of the types of Access- list which is mostly used as it can distinguish IP traffic therefore the whole traffic will not be permitted or

denied like in standard access-list. These are the ACL that uses both source and destination IP addresses and also the port numbers to distinguish IP traffic. In this type of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.



R1 (config)# ip access-list extended blockacl
R1 (config-ext-nacl)# deny tcp 172.16.40.0 0.0.0.255
172.16.50.0

0.0.0.255 eq 21
R1(config-ext-nacl)# deny tcp any 172.16.50.0 0.0.0.255 eq 23 **R1(config-extnacl)#** permit ip any

.

EXPERIMENT NO. 14

Aim:

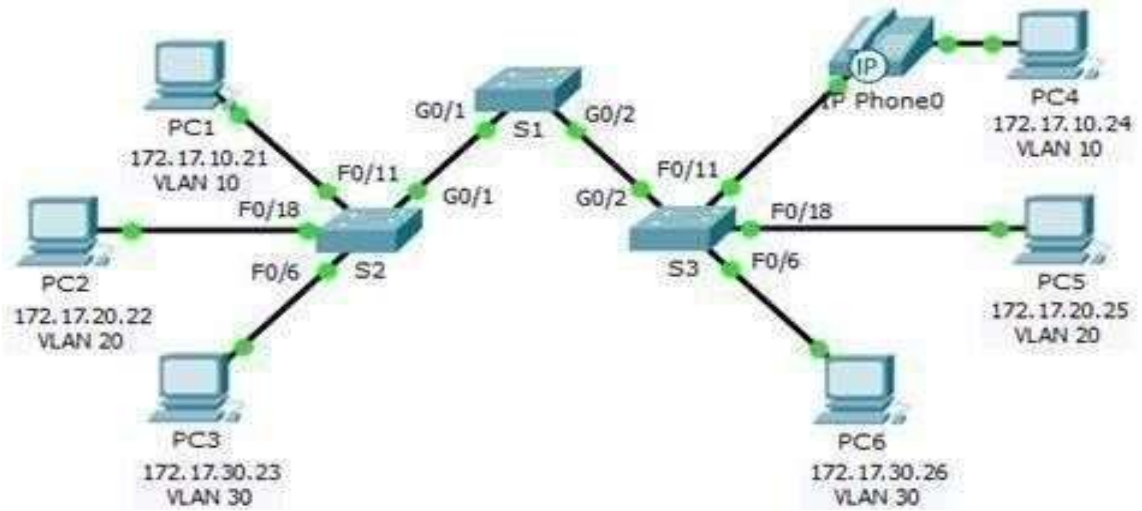
Creating and managing communication through VLAN in computer networks.

Theory:

VLAN is Virtual LAN. A VLAN is a broadcast domain . By default hosts in single VLAN communicates to each other . But host in different VLANS won't communicate to each other , to ensure communication between different VLan's host routing between VLAN's is mandatory for Configuring routing between VLAN layer3 device is required .

Two separate VLAN's can communicate with each other through layer 3 like a router. Devices on a VLAN communicate with each other using layer-2. Layer-3 must be used to communicate between separate layer-2 domains.

When a host on one VLAN wants to send something to a host on another VLAN, it must use a layer-3 (e.g. IP) address. The host will use layer-2 to send the frames to its defined gateway (router). The router will strip off the layer-2 frame and inspect the layer-3 packet for the destination layer-3 address. The router will then look up the next hop for the layer-3 address. It will then create a new layer-2 frame for the layer-3 packet based on the layer-2 LAN on the interface where it needs to send the packet for the next hop. Other routers which may be in the path to the end LAN will repeat this process until the frame is placed on the final VLAN, where the receiving host gets the frame.



EXPERIMENT NO. 15

AIM: To apply NAT (network address translation) static.

Theory:

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Procedure:

1) Set up a network of at least three computers, each with a unique IP address assigned by the local network router. Determine the IP addresses of each computer in the network. You can do this by opening the command prompt or terminal and typing "ipconfig" or "ifconfig" respectively.
2) Choose one computer to act as the NAT gateway. This will be the computer that connects to the internet, and all other computers in the network will connect to it to access the internet. Configure the NAT gateway to use static NAT. This means that each computer in the network will be assigned a unique public IP address that will be used to communicate with devices outside of the local network.
3) Configure the NAT gateway to assign a unique private IP address to each computer in the network. The private IP address will be used to communicate between devices within the local network.
4) Test the network by attempting to access the internet from each computer in the network. If successful, each computer should have a unique public IP address, and all traffic should be able to pass through the NAT gateway. Monitor network traffic to ensure that all devices are communicating as expected. Use network monitoring tools to track traffic patterns and identify any potential security vulnerabilities.
5) Evaluate the performance of the network with NAT static enabled. Compare the speed and reliability of the network before and after implementing NAT static.

6) Document the network configuration, including IP addresses, router settings, and any other relevant details. This documentation will be helpful for troubleshooting and future network management.