NETAJI SUBHAS UNIVERSITY OF TECHNOLOGY

NEW DELHI

COMPUTER NETWORKS

EIECC16

Mini Projects File

EIOT

(Semester V)

SUBMITTED TO:

Mr. Shailesh Mishra

SUBMITTED BY:

Deepanshu

2020UEI2810

INDEX

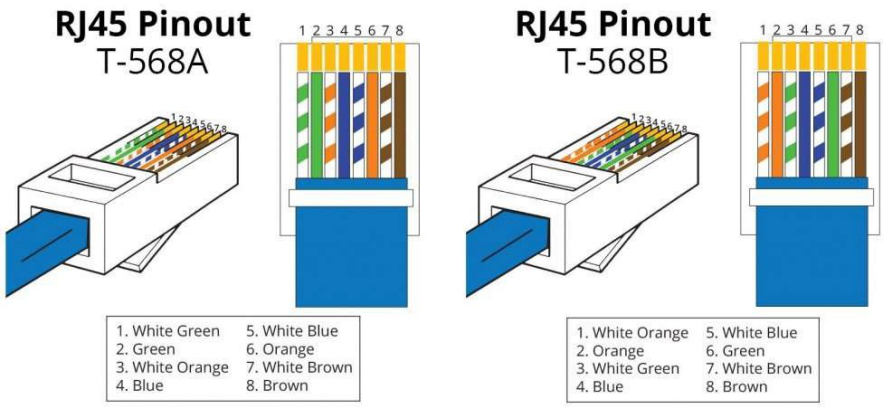
Mini Project No.-1

Aim: Study of cables and connectors in computer network, design and construct straight and cross LAN cable.

Apparatus: Cables, Crimping tool.

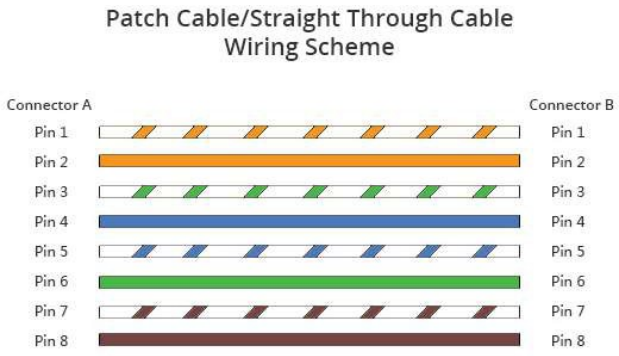
Theory:

T-568A vs. T-568B:



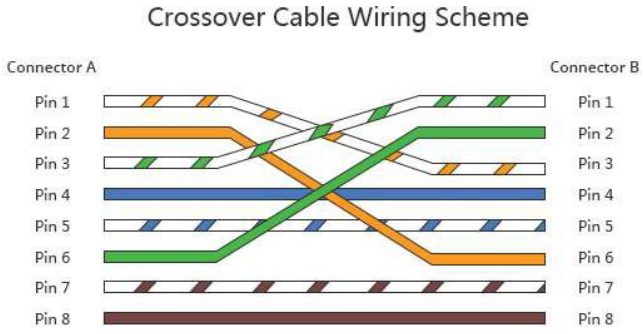
Before talking about patch cable and crossover cable, it's very necessary to learn about the T-568A and T-568B standard. With regard to these two patch cable wiring schemes, there are two different connectivity forms. The T-568B wiring scheme is by far the most common, though many devices support the T-568A wiring scheme as well. If both ends of the patch cords are wired on the basis of one standard, it is a straight through connection. Both the standards can be used for straight through cable. If not, it is a crossover connection. Some networking applications require an Ethernet crossover cable, which has a T-568A connector on one end and a T-568B connector on the other. This type of cable is typically used for direct computer-to-computer connections. The following section will introduce the straight through cable (or patch cable) and crossover cable in details.

Patch Cable:



Many networking professionals use the term patch cable to refer to any kind of straight through cable. So, a patch cable is often called a straight through cable. In other words, patch cable does not change or swap along its way. Both ends use the same wiring standard: T-568A or T-568B. So, both side (connector A and connector B) of patch cable have wire arrangement with same patch cable colors (as shown in the following picture). These patch cables are widely used for connecting the computer to the switches, hubs, or routers.

Crossover cable:



Crossover cable, as the name suggests, cross over or swap on its way when coming from one end to the other. Unlike patch cable, crossover cable uses two different wiring standards on both end: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. Both side (connector A and connector B) of crossover cable have wire arrangement with different color, and the wires that come out of the connector A should match the correct pin at the connector B.

Result: We studied about cables and connectors and analyzed straight and cross LAN cables

Mini Project No.-2

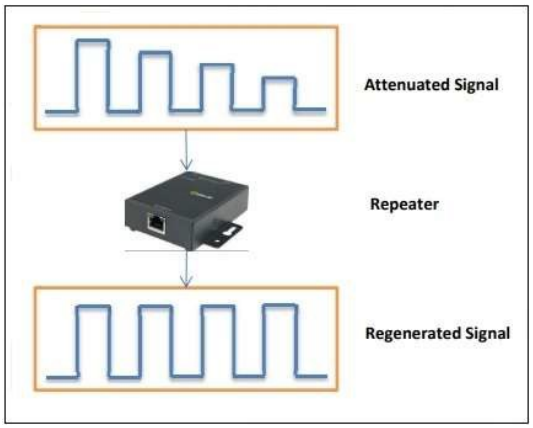
Aim: Study of following Network Devices in Detail:

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

Apparatus: Laptop, Cisco Packet Tracer.

Theory:

Repeater:



Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.

Types of Repeaters:

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- **Analog Repeaters** − They can only amplify the analog signal.
- **Digital Repeaters** − They can reconstruct a distorted signal.

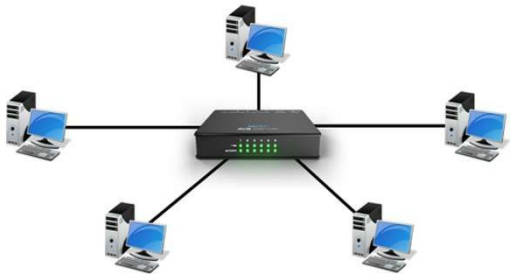
According to the types of networks that they connect, repeaters can be categorized into two types −

- **Wired Repeaters** − They are used in wired LANs.
- **Wireless Repeaters** − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- **Local Repeaters** − They connect LAN segments separated by small distance.
- **Remote Repeaters** − They connect LANs that are far from each other.

Hub:



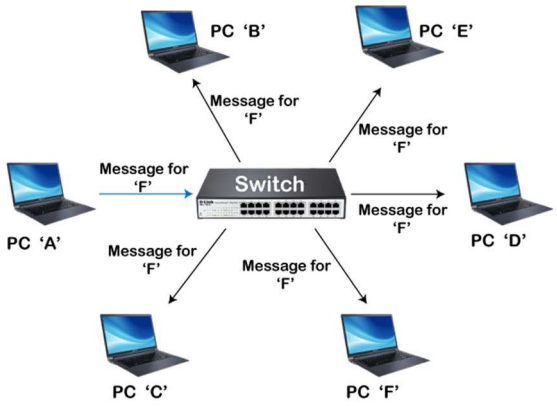
A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices.

Network hubs are best suited for small, simple local area network (LAN) environments. Hubs cannot provide routing capabilities or other advanced network services. Because they operate by forwarding packets across all ports indiscriminately, network hubs are sometimes referred to as "dumb switches."

Types of network hubs:
There are two types of network hubs: active and passive. A third designation, intelligent hubs, is synonymous with a switch.

- **Active hubs** repeat and strengthen incoming transmissions. They are also sometimes referred to as repeaters.
- **Passive hubs** simply serve as a point of connectivity, without any additional capabilities.

Switch:



A switch is a device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended. Each networked device connected to a switch can be identified by its network address, allowing the switch to direct the flow of traffic maximizing the security and efficiency of the network.

A switch is more intelligent than an Ethernet hub, which simply retransmits packets out of every port of the hub except the port on which the packet was received, unable to distinguish different recipients, and achieving an overall lower network efficiency.

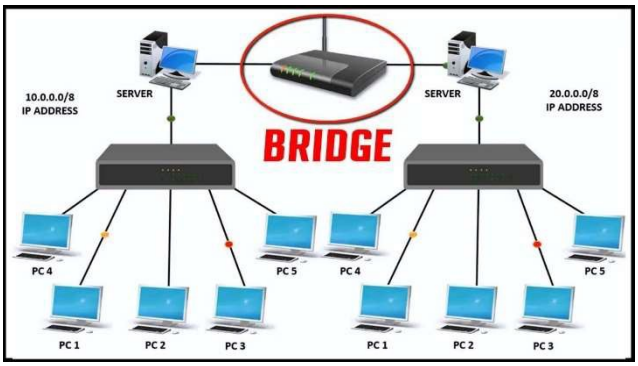
Types of Switches:

- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices need to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organizations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in

growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.

- **LAN Switch** − Local Area Network (LAN) switches connect devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

Bridge:



Bridges are used to connect two subnetworks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.

Types of bridges:

- **Transparent Bridges**

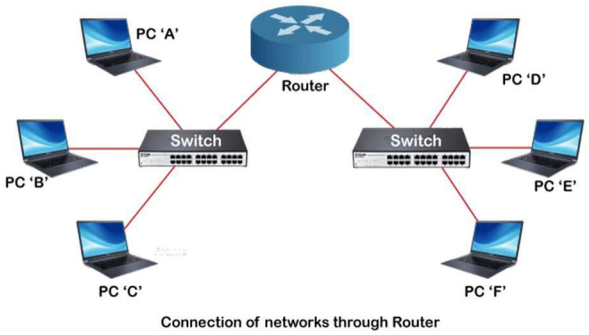
It is also called learning bridges. Bridge constructs its table of terminal addresses on its own as it implements connecting two LANs. It facilitates the source location to create its table. It is self-updating. It is a plug and plays bridge.

- **Source Routing Bridge**

This sending terminal means the bridges that the frames should stay. This type of bridge is used to prevent looping problem.

Router:

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

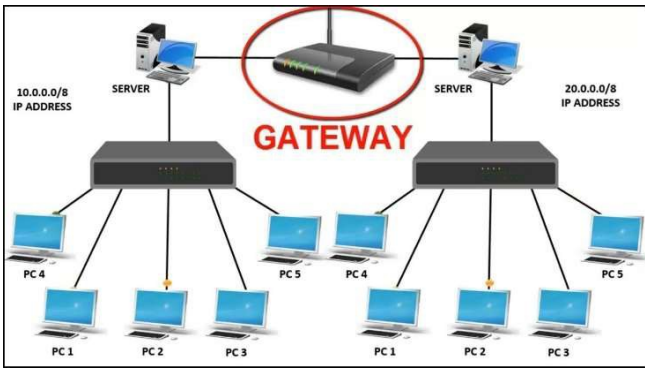


Connection of networks through Router

Types of Routers:

- **Wireless Router** − They provide Wi-Fi connection Wi-Fi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
- **Broadband Routers** − They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- **Core Routers** − They can route data packets within a given network, but cannot route the packets between the networks. They help to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
- **Edge Routers** − They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.
- **Brouters** − Brouters are specialized routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

Gate Way:



A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e., network layer of the OSI (open systems interconnection) model.

However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

Types of Gateways:

- **Unidirectional Gateways** − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
- **Bidirectional Gateways** − They allow data to flow in both directions. They can be used as synchronization tools.

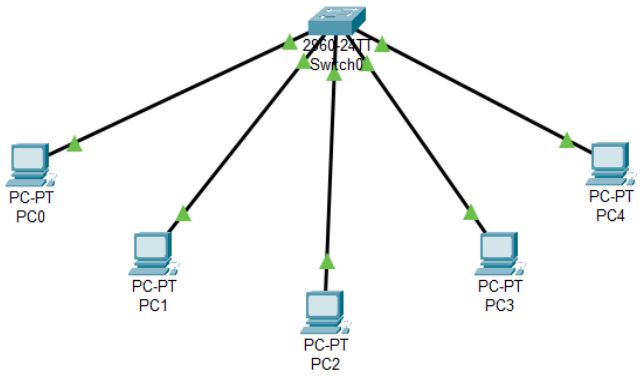
Result: We studied about all the network devices in detail.

Mini Project No.-3

Aim: Connect the computers in Local Area Network, and Study of basic network command and Network configuration commands.

Apparatus: Laptop, Cisco Packet Tracer.

Experiment:



IP Addresses for:

PC0 – 192.168.1.1

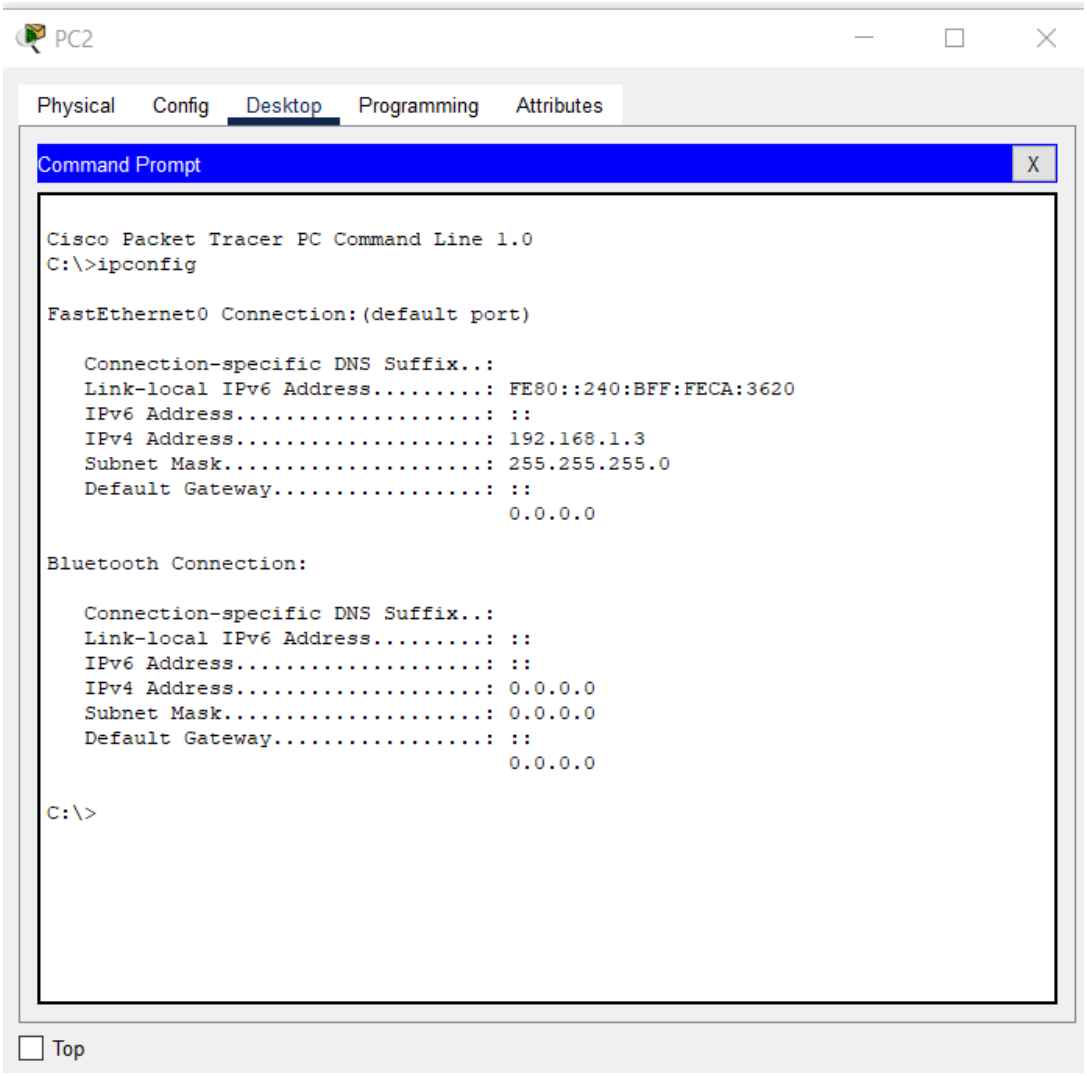
PC1 – 192.168.1.2

PC2 – 192.168.1.3

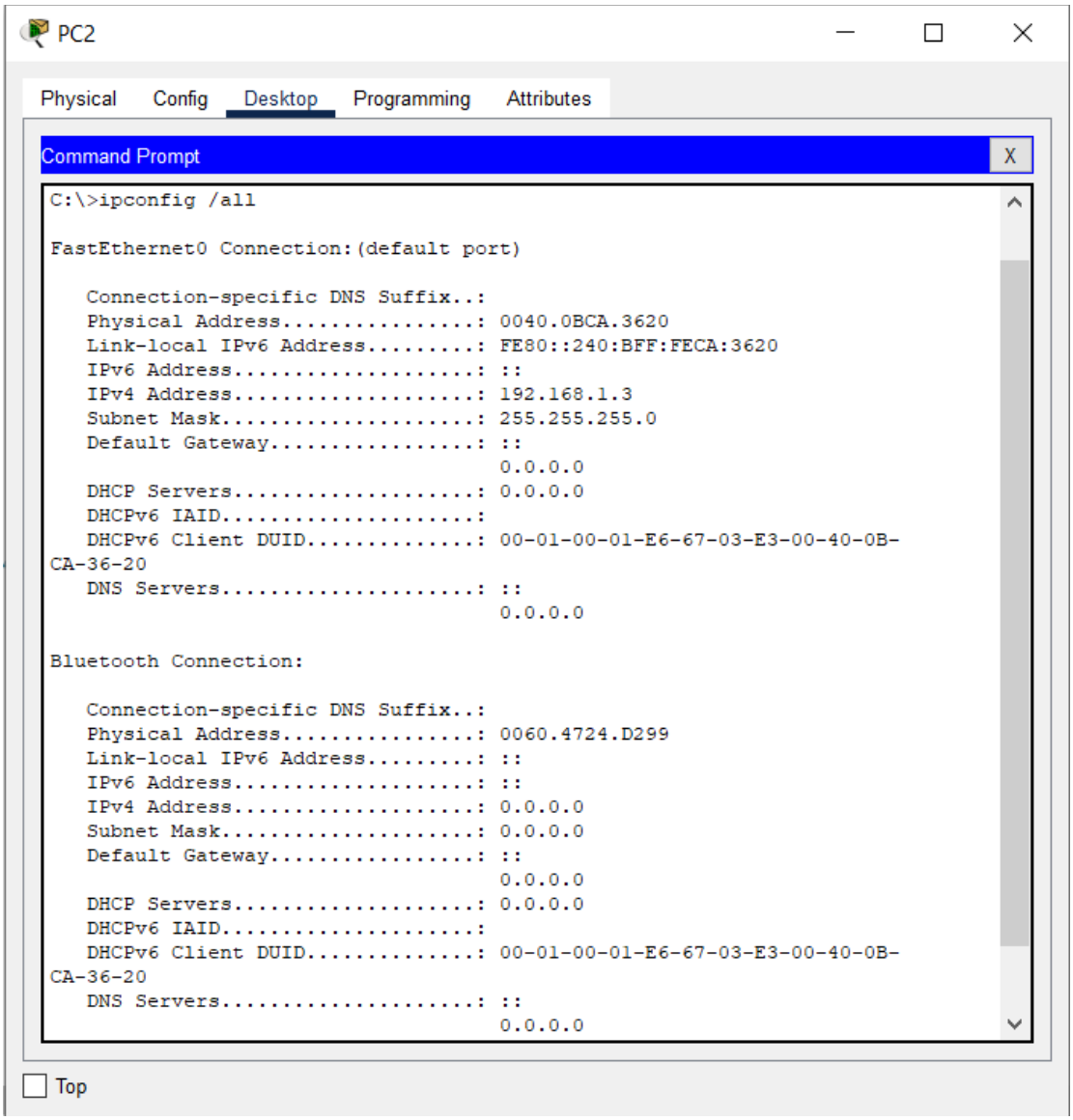
PC3 – 192.168.1.4

PC4 – 192.168.1.5

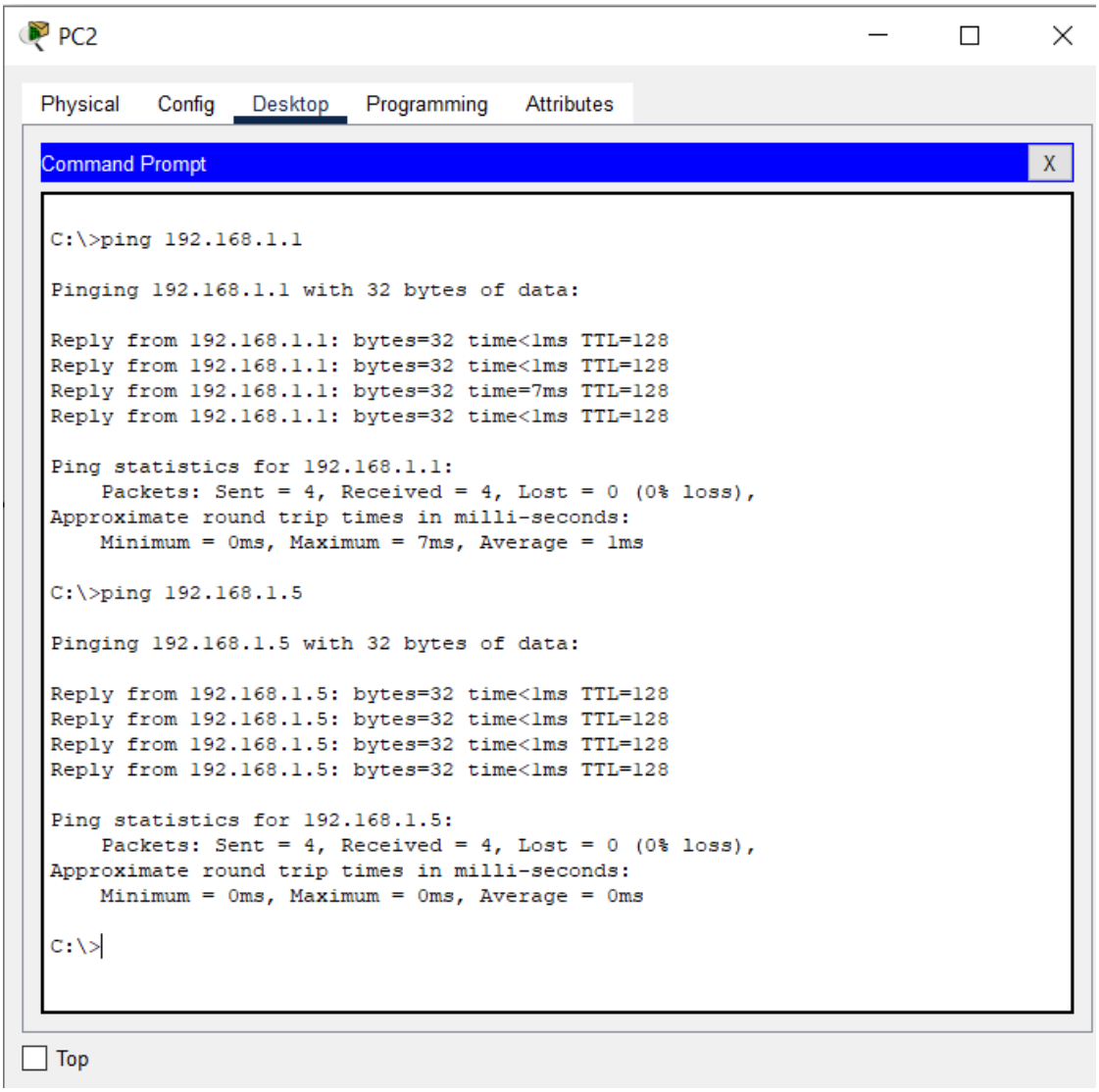
IPCONFIG:


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::240:BFF:FECA:3620
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
0.0.0.0
Bluetooth Connection:
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
C:\>
Top

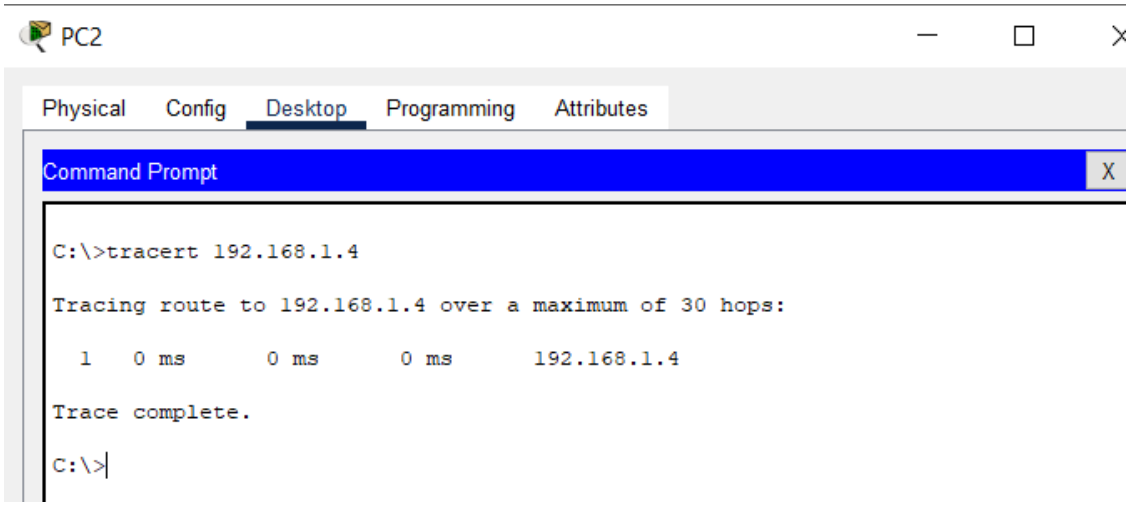
IPCONFIG /ALL:



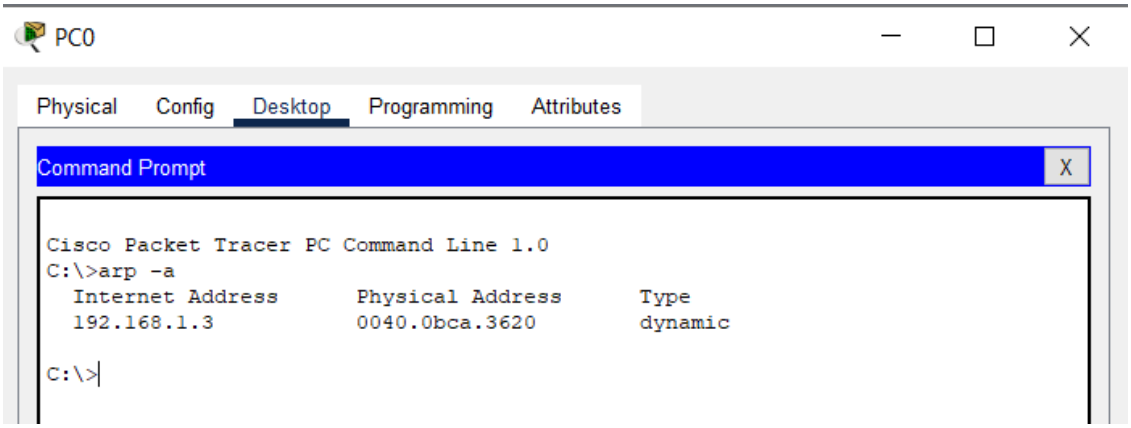
PING:


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=7ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 1ms
C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

TRACERT:



ARP:



Result: A Local Area Network was successfully created using switch and some basic networking commands were studied.

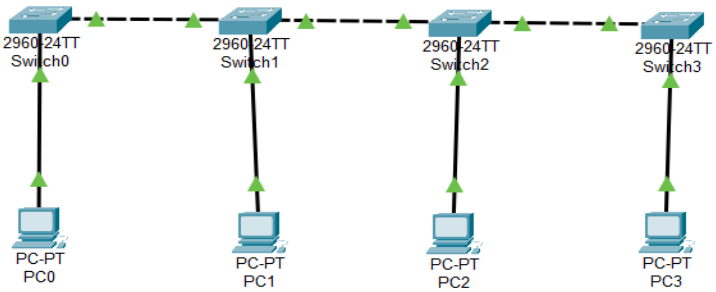
Mini Project No.-4

Aim: Configure and analyze bus, ring, star, mesh, and hybrid network topology with wired vs wireless networks.

Apparatus: Laptop, Cisco Packet Tracer.

Experiment:

Bus Topology: In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time.



IP Addresses for:

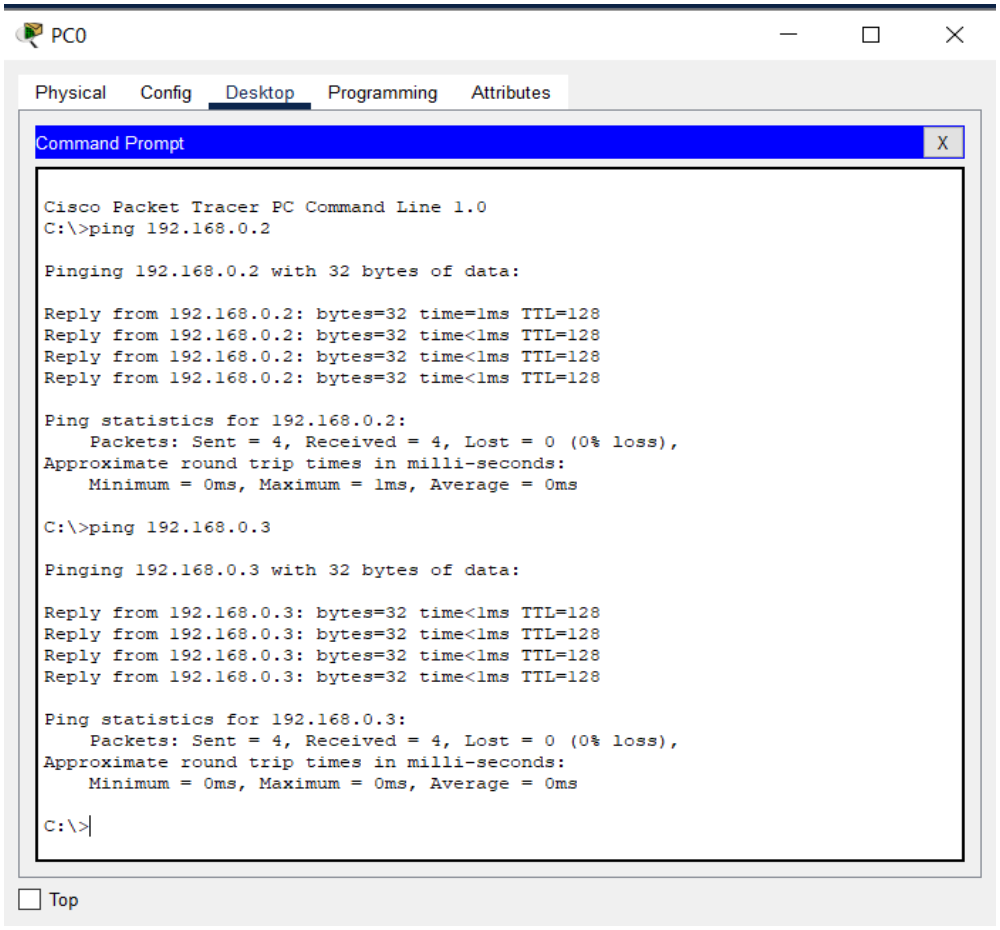
PC0 – 192.168.0.1

PC1 – 192.168.0.2

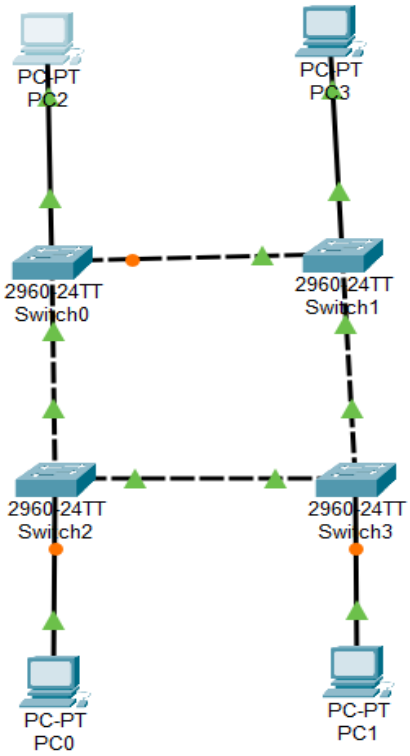
PC2 – 192.168.0.3

PC3 – 192.168.0.4

Ping:


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

Ring Topology: In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.



IP Addresses for:

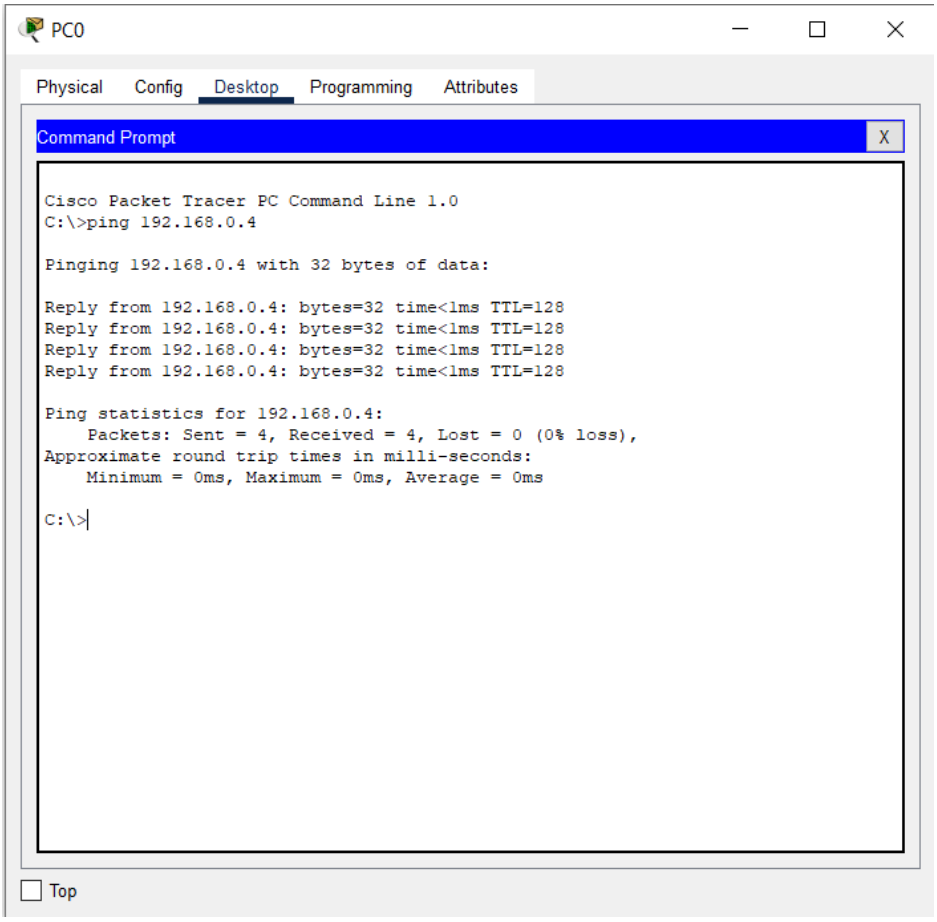
PC0 – 192.168.0.1

PC1 – 192.168.0.2

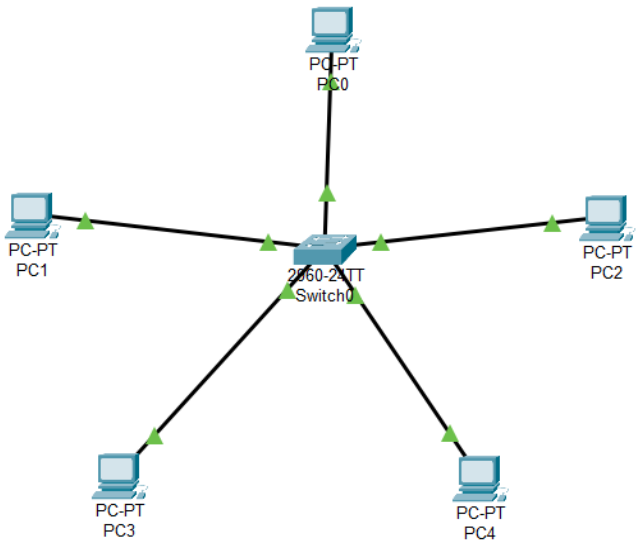
PC2 – 192.168.0.3

PC3 – 192.168.0.4

Ping:


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.4
Pinging 192.168.0.4 with 32 bytes of data:
Reply from 192.168.0.4: bytes=32 time<1ms TTL=128
Reply from 192.168.0.4: bytes=32 time<1ms TTL=128
Reply from 192.168.0.4: bytes=32 time<1ms TTL=128
Reply from 192.168.0.4: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

Star Topology: All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point-to-point connection between hosts and hub.



IP Addresses for:

PC0 – 192.168.0.1

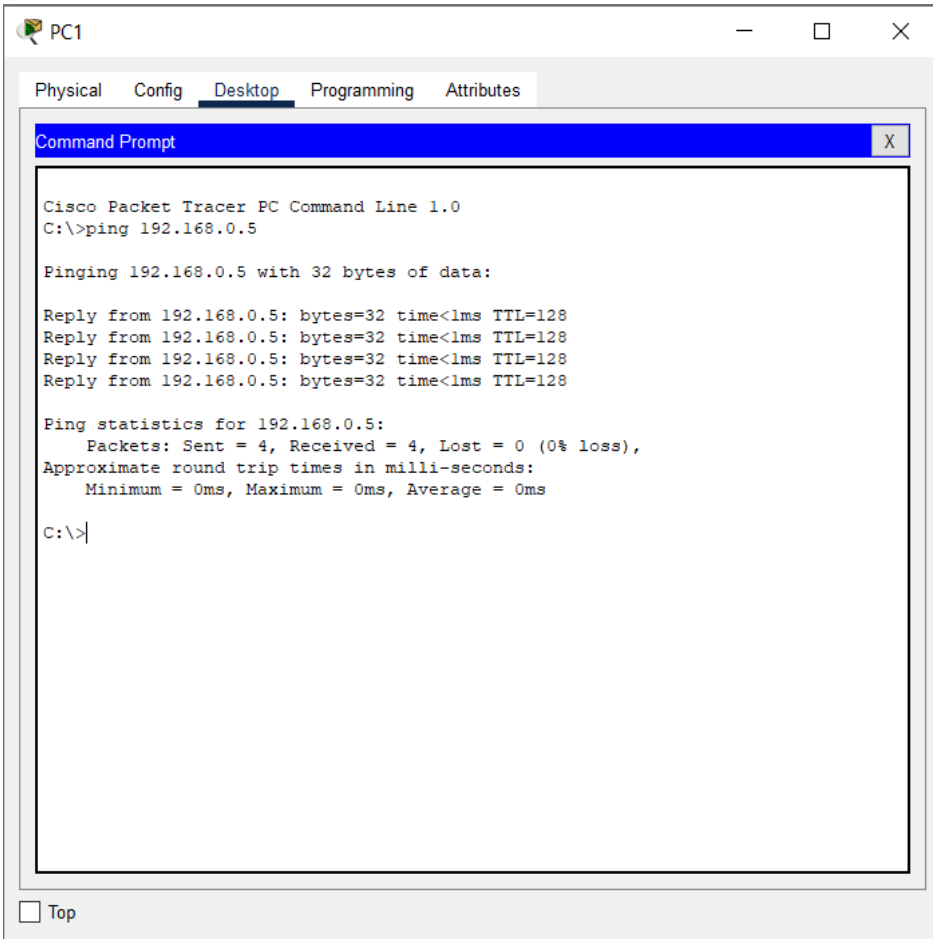
PC1 – 192.168.0.2

PC2 – 192.168.0.3

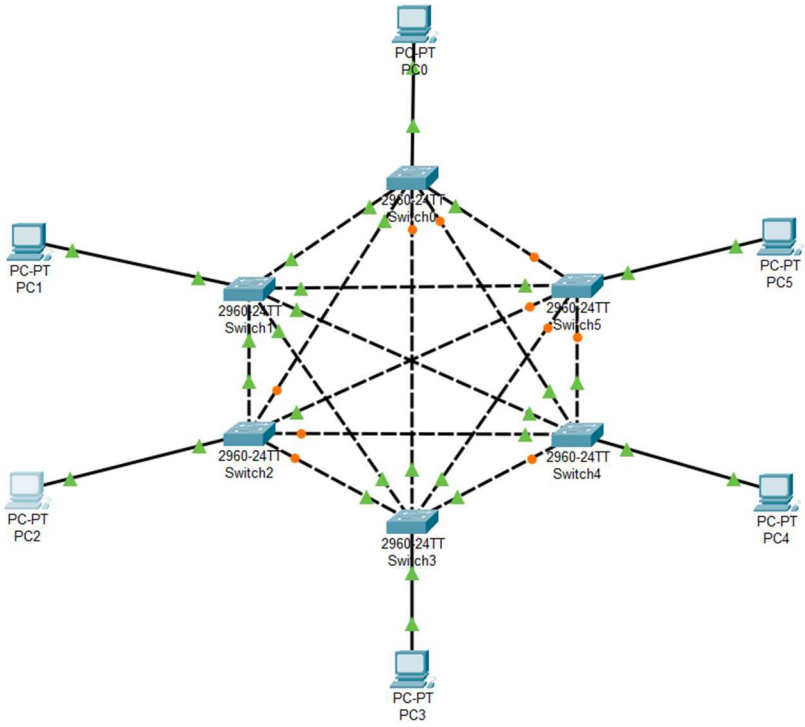
PC3 – 192.168.0.4

PC4 – 192.168.0.5

Ping:


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.5
Pinging 192.168.0.5 with 32 bytes of data:
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

Mesh Topology: In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



IP Addresses for:

PC0 – 192.168.0.1

PC1 – 192.168.0.2

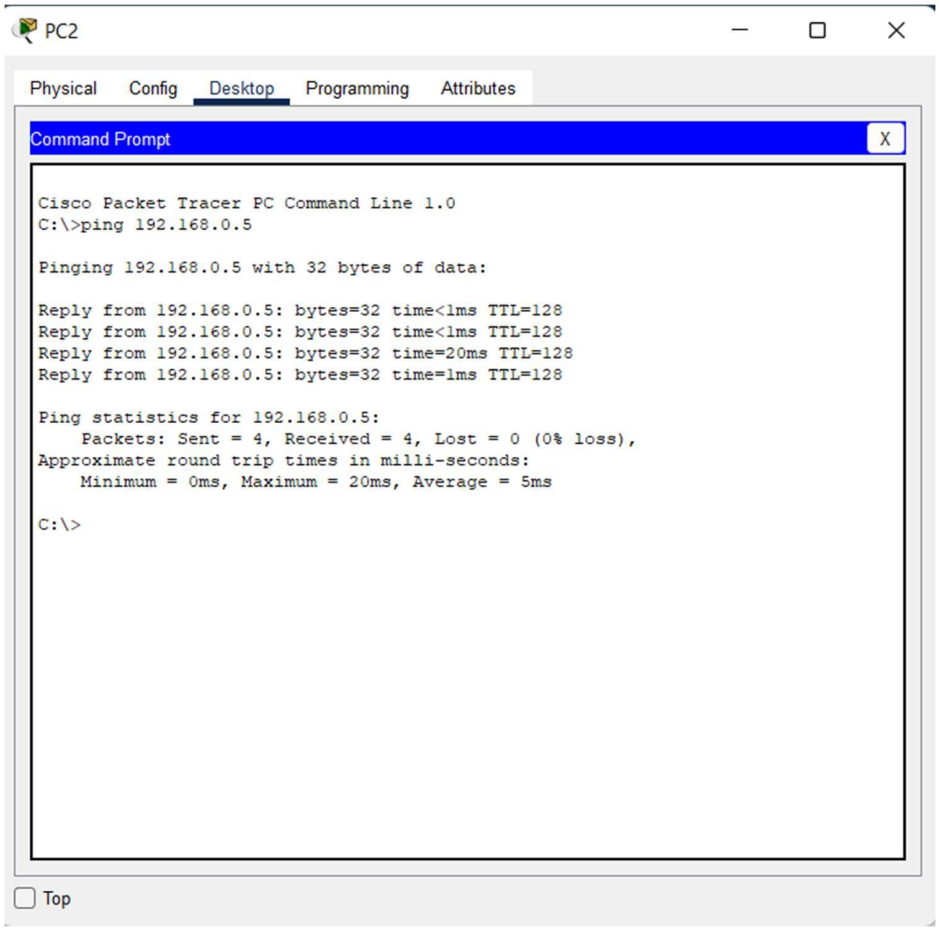
PC2 – 192.168.0.3

PC3 – 192.168.0.4

PC4 – 192.168.0.5

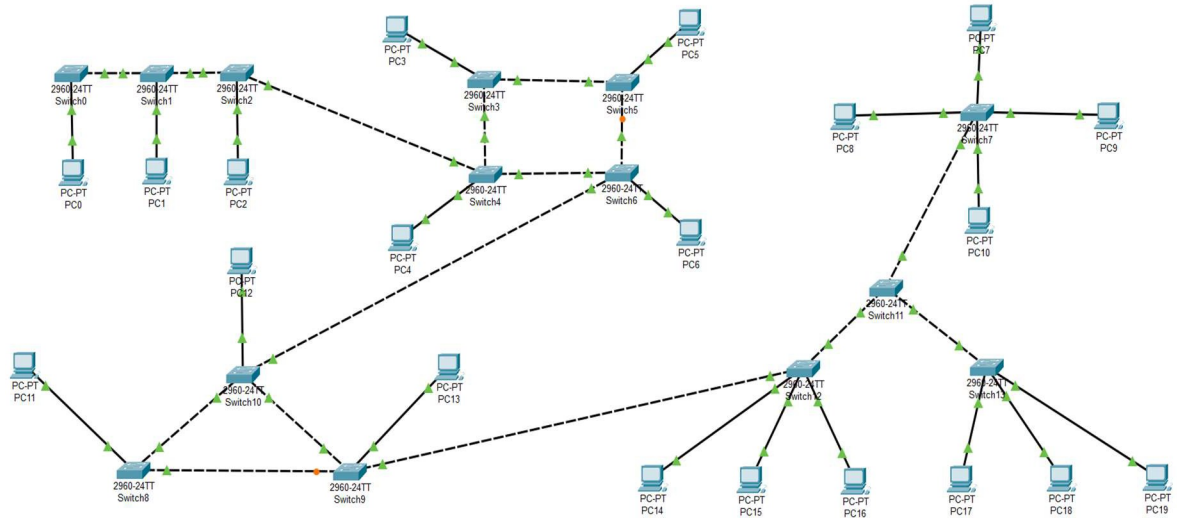
PC5 – 192.168.0.6

Ping:


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.5
Pinging 192.168.0.5 with 32 bytes of data:
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time=20ms TTL=128
Reply from 192.168.0.5: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 20ms, Average = 5ms
C:\>
Top

Hybrid Topology:

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.
Combination of 5 topologies i.e., bus, ring, star, mesh, tree with a total of 20 computers.



IP Addresses for:

PC0 – 192.168.0.1

PC1 – 192.168.0.2

PC2 – 192.168.0.3

PC3 – 192.168.0.4

PC4 – 192.168.0.5

PC5 – 192.168.0.6

PC6 – 192.168.0.7

PC7 – 192.168.0.8

PC8 – 192.168.0.9

PC9 – 192.168.0.10

PC10 – 192.168.0.11

PC11 – 192.168.0.12

PC12 - 192.168.0.13

PC13 - 192.168.0.14

PC14 - 192.168.0.15

PC15 - 192.168.0.16

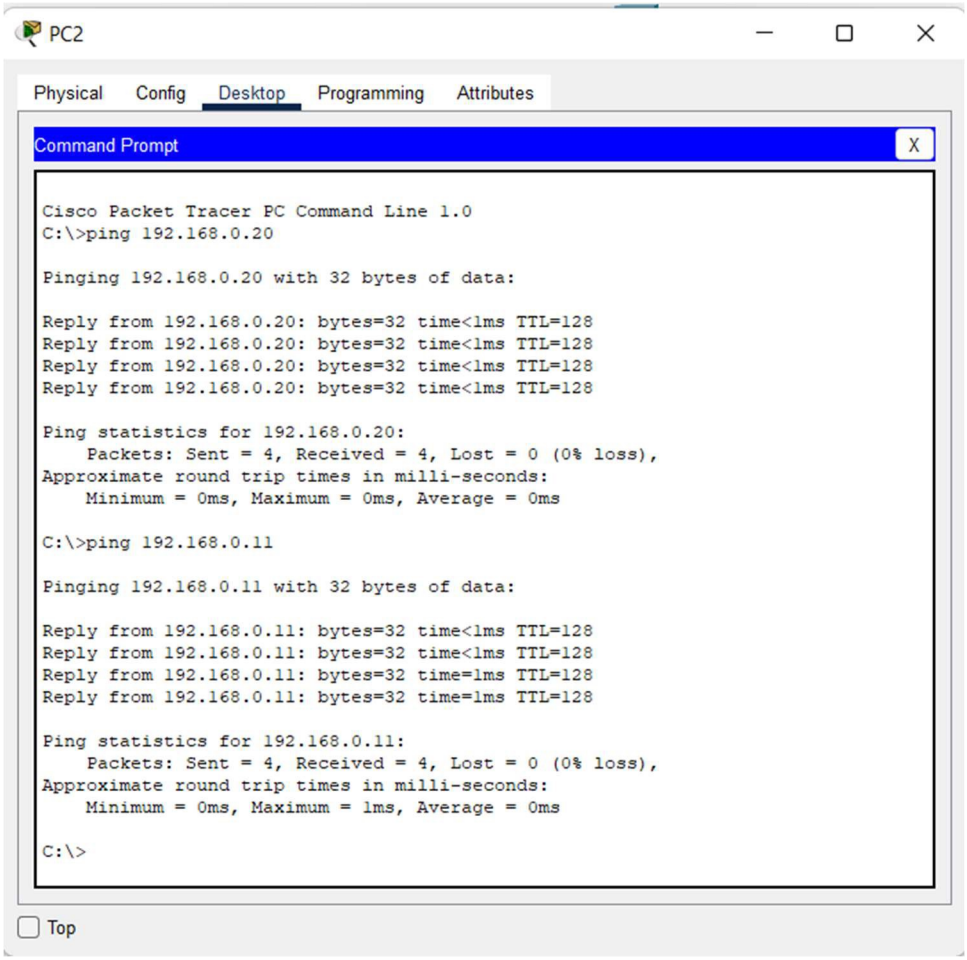
PC16 - 192.168.0.17

PC17 - 192.168.0.18

PC18 - 192.168.0.19

PC19 – 192.168.0.20

Ping:



Result: Bus, ring, star, mesh, hybrid topologies were configured and analyzed.

Mini Project No.-5

Aim: Study of protocol of encapsulation and authentication protocol in computer networking.

Apparatus: Laptop, Cisco Packet Tracer.

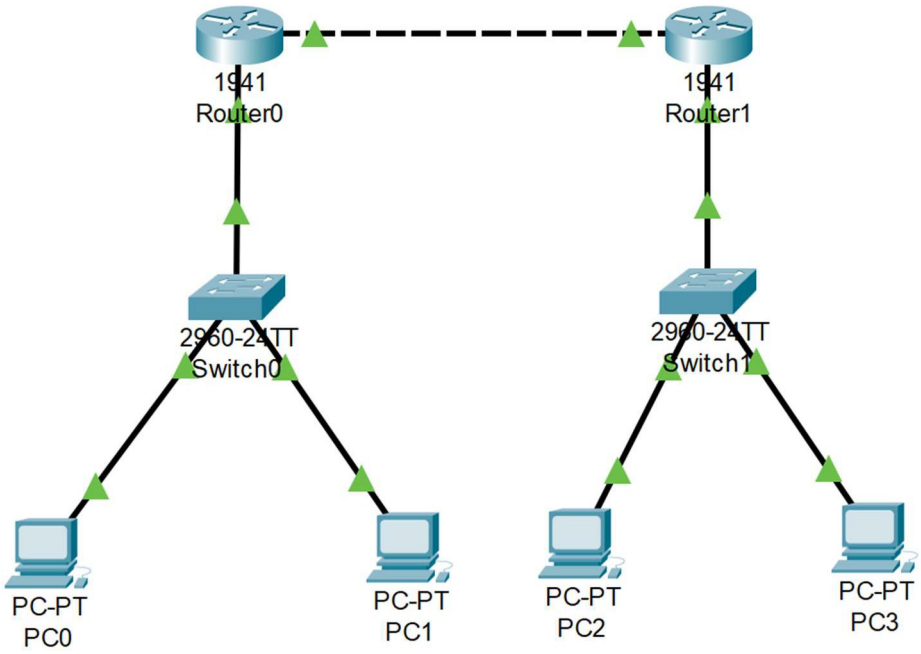
Experiment:

Point-to-Point Protocol (PPP) is basically a Wide Area Network (WAN) protocol that performs or works at layer 2 by simply encapsulating frames for transmission or transferring over different physicals links or connections like serial cables, cell phones, fiber optic cable among others, etc.

Encapsulation is basically a process in which lower-layer protocol basically receives data from higher layer protocol and then further places this data portion of its frame.

In simple words, we can say the encapsulation is process of enclosing one type of packing with help of other types of packets. PPP generally provides encapsulation so that various protocols at the network get supported simultaneously. PPP connections also deliver or transmit packets in sequence and provide full-duplex simultaneous bi-directional operation. PPP usually encapsulates any of the network layer packets in its frame that makes it possible for PPP layer three protocol to become independent and even capable of carrying multiple-layer three packets through a single link or connection.

PPP Encapsulation is also required to disambiguate multiprotocol datagrams i.e., removal of ambiguity to make the multiprotocol datagrams clear and easy to be understood. PPP puts data in a frame and transmit it through PPP connection or link. A frame is basically defined as a unit of transmission in Data Link Layer (DLL) of the OSI protocol stack. To form encapsulation, a total of 8-bytes is required.



Default Gateway for Switch0 – 192.168.1.1

- IP address of PC0 – 192.168.1.2 (255.255.255.0)
- IP address of PC1 – 192.168.1.3 (255.255.255.0)

Default Gateway for Switch1 – 192.168.2.1

- IP address of PC2 – 192.168.2.2 (255.255.255.0)
- IP address of PC3 – 192.168.2.3 (255.255.255.0)

CLI commands for Router0:

Enable

Configure terminal

Interface fastethernet 0/0/0

Ip address 192.168.1.1 255.255.255.0

No shutdown

Exit

Interface fastethernet 0/0/1

Ip address 192.168.3.1 255.255.255.0

No shutdown

Exit

Ip route 192.168.2.0 255.255.255.0 fastethernet 0/0/1

CLI commands for Router1:

Enable

Configure terminal

Interface fastethernet 0/0/0

Ip address 192.168.2.1 255.255.255.0

No shutdown

Exit

Interface fastethernet 0/0/1

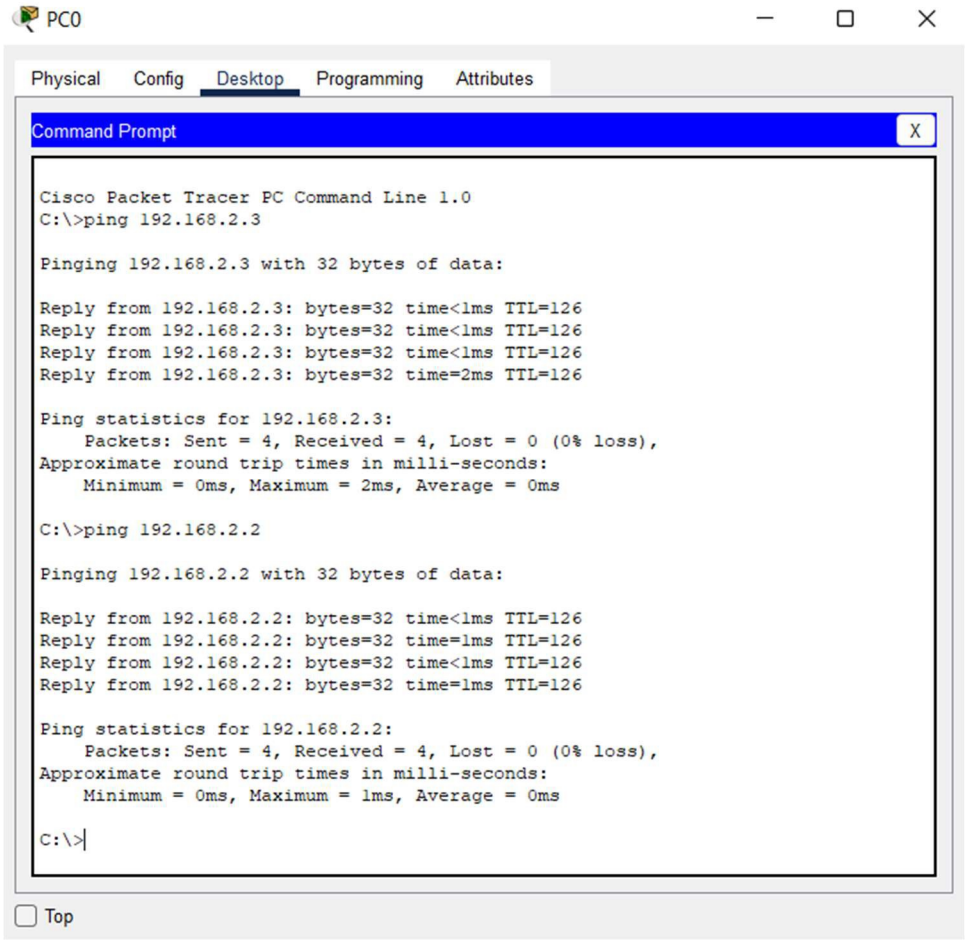
Ip address 192.168.3.2 255.255.255.0

No shutdown

Exit

Ip route 192.168.1.0 255.255.255.0 fastethernet 0/0/1

Ping:



Result: We studied the protocol of encapsulation and authentication protocol in computer networking.

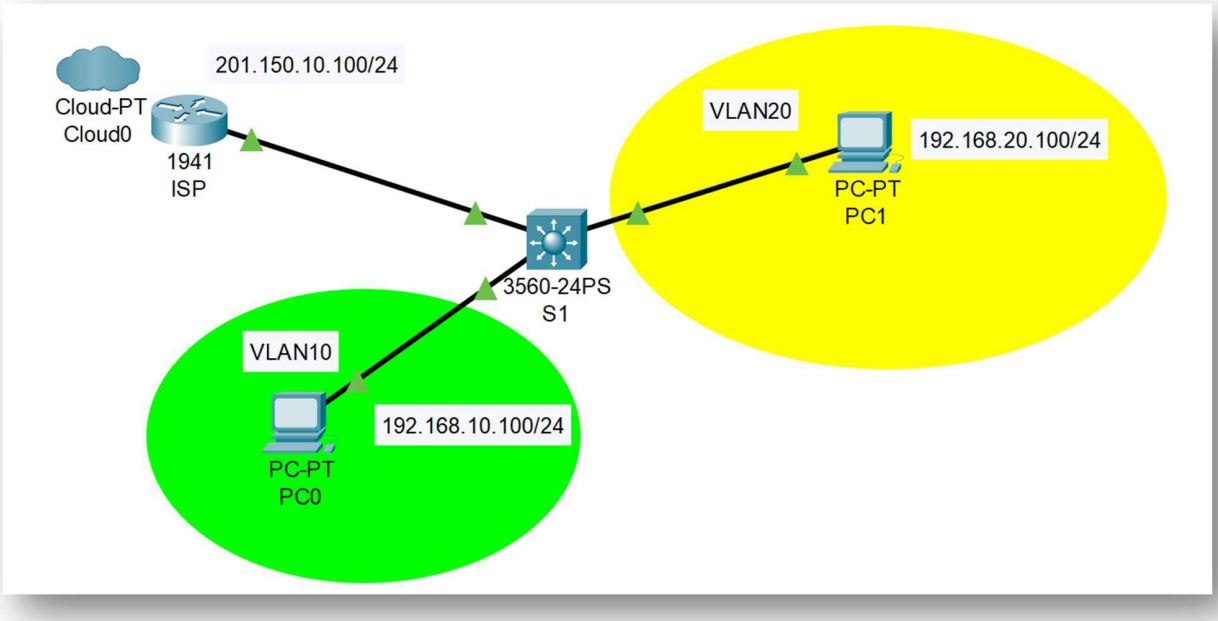
Mini Project No.-6

Aim: To Perform multilayer Switching in computer network.

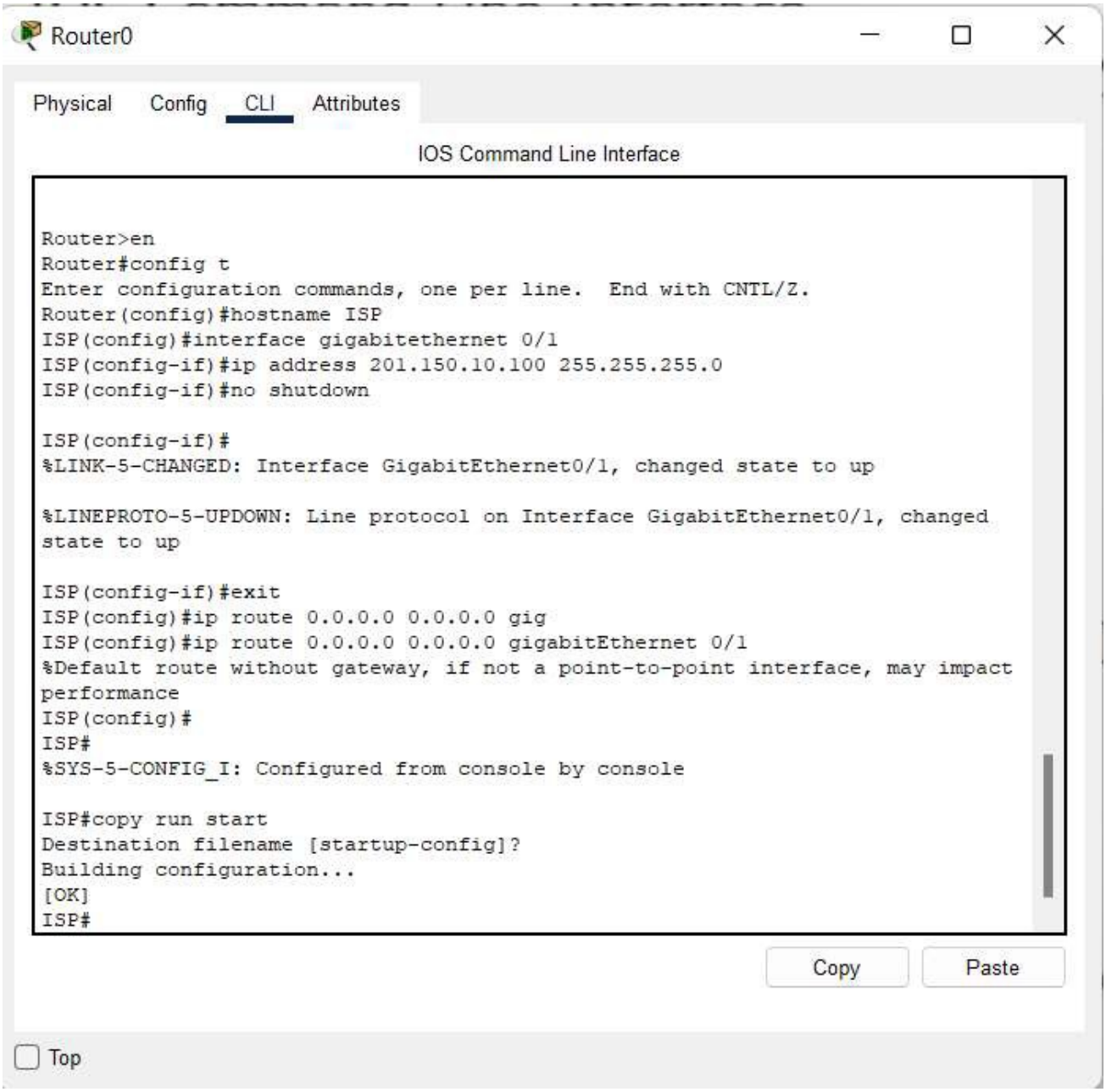
Apparatus: Laptop, Cisco Packet Tracer.

Experiment:

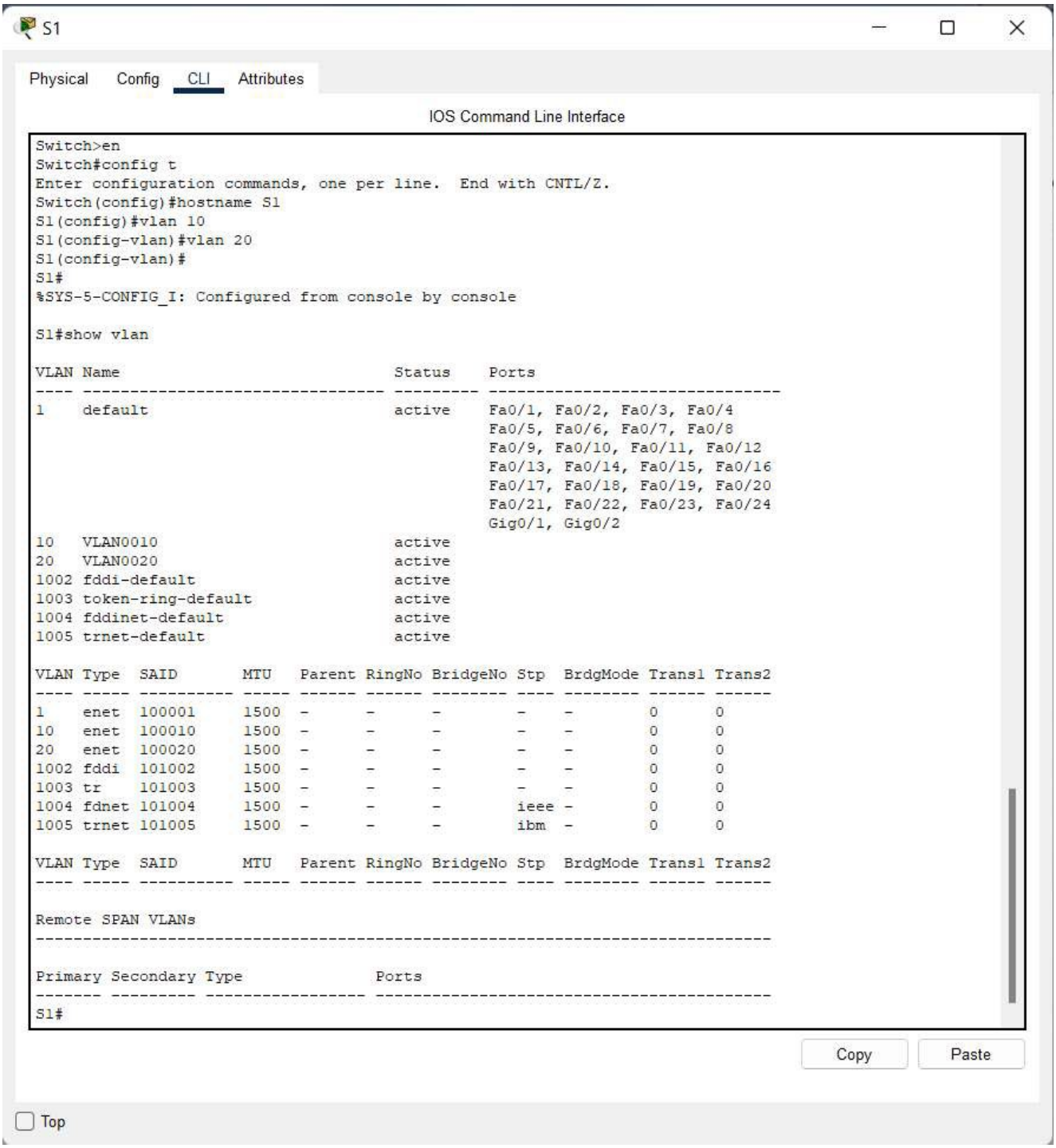
A multilayer switch is a network device that has the ability to operate at higher layers of the OSI reference model, unlike the Data Link Layer (DLL) traditionally used by switches. A multilayer switch can perform the functions of a switch as well as that of a router at incredibly fast speeds. A switch traditionally inspects frames, while a multilayer switch inspects deeper into the protocol description unit (at packet or even at segment level). Multilayer switches use ASIC hardware circuits to perform routing functions. This differs from typical routers, which reside on a microprocessor and use applications running on it to perform their routing operations.



Configuring Router:



Configuring Switch:



D X

Physical Config CU A.ttributes

10S Command Line Interface

```
SH
SHconfig t
Enter configuration commands, one per line. End with CNTL/2.
Sl(config)#interface fast
Sl(config)#interface fastEthernet 0/1
Sl(config-if)#switchport mode access
Sl(config-if)#switchport access vlan 10
Sl(config-if)#interface fastEthernet 0/2
Sl(config-if)#switchport mode access
Sl(config-if)#switchport access vlan 20
Sl(config-if)#exit
Sl(config)#
Sl(config)#interface vlan 10
Sl(config-if)#
%LINK-5-CHANGED: Interface Vlanl0, changed state to up

%LINEPROT0-5-UPDOWN: Line protocol on Interface Vlanl0, changed state to up

Sl(config-if)#ip address 192.168.10.l 255.255.255.0
Sl(config-if)#no shut
Sl(config-if)#interface vlan 20
Sl(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROT0-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

Sl(config-if)#ip address 192.168.20.l 255.255.255.0
Sl(config-if)#no shut
Sl(config-if)#
SH
%SYS-5-CONFIG I: Configured from console by console

Sl#show run
Building configuration...

Current configuration : 1454 bytes

version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname Sl
```

Copy Paste

Q Top

D X

Physical Config CU Attributes

10S Command Line Interface

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate

interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19
```

Copy Paste

Q Top

D X

Physical Config CU Attributes

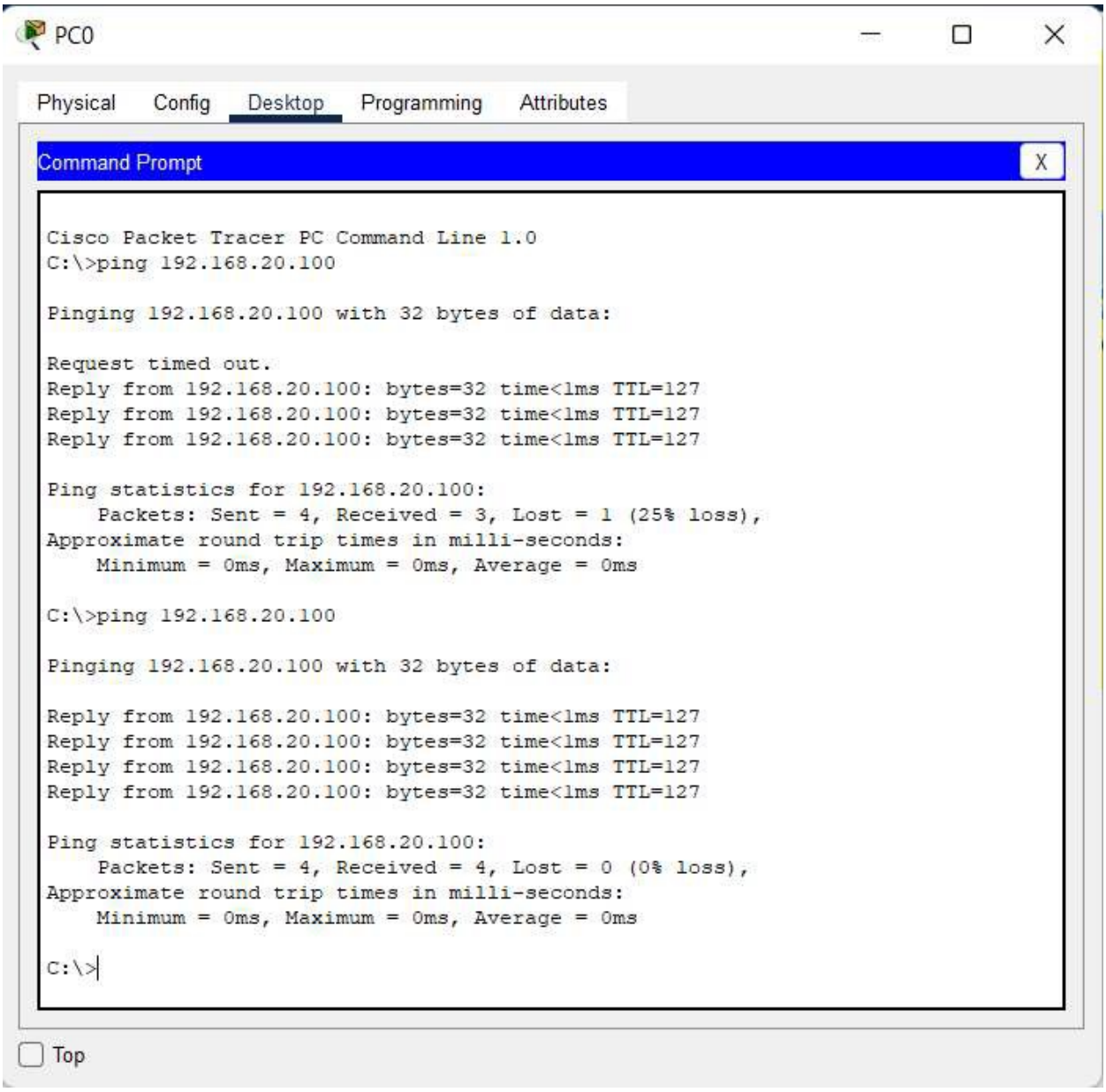
10 S Com m and Line Interface

```
 shutdown

interface Vlan1O
 mac-address 0050.0f82.a101
 ip address 192.168.10.1 255.255.255.0

interface Vlan20
 mac-address 0050.0f82.a102
 ip address 192.168.20.1 255.255.255.0

ip classless

ip flow-export version 9









line con O

line aux O

line vty O 4
 login




end


SU
SU
SU
SU
SU
SU
SU
SU
SU
SU config t
Enter configuration commands, one per line. End with CNTL/2.
Sl(config)#ip routing
Sl(config)ti
```

Copy Paste

Q Top

Ping:



Result: Multilayer switching was successfully performed in computer networks.

Mini Project No.-7

Aim: Configuring IP routing using routing information protocol.

Apparatus: Laptop, Cisco Packet Tracer.

Experiment:

Routing Information Protocol (RIP) is a distance-vector routing protocol. Routers running the distance-vector protocol send all or a portion of their routing tables in routing-update messages to their neighbors

Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

Hop Count:

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

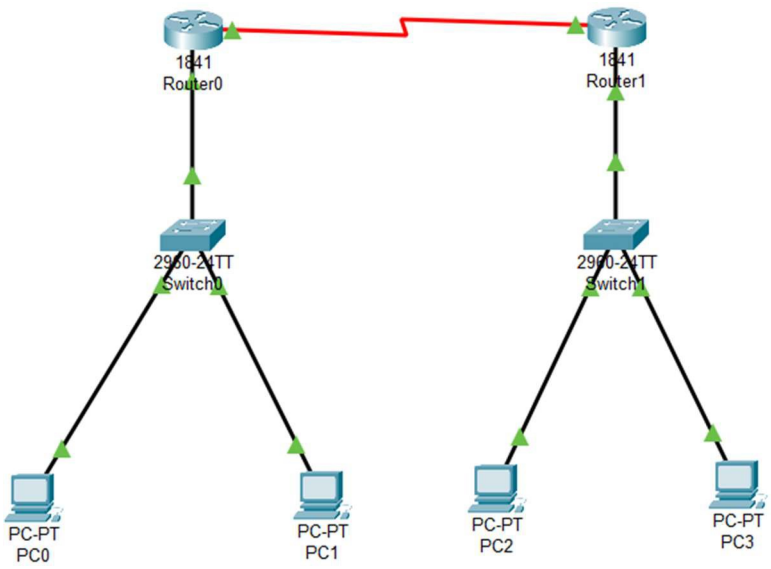
Features of RIP:

1. Updates of the network are exchanged periodically.

2. Updates (routing information) are always broadcast.

3. Full routing tables are sent in updates.

4. Routers always trust routing information received from neighbor routers. This is also known as Routing on rumors.



Default Gateway for Switch0 – 192.168.1.1

- IP address of PC0 – 192.168.1.2 (255.255.255.0)
- IP address of PC1 – 192.168.1.3 (255.255.255.0)

Default Gateway for Switch1 – 192.168.2.1

- IP address of PC2 – 192.168.2.2 (255.255.255.0)
- IP address of PC3 – 192.168.2.3 (255.255.255.0)

CLI commands for Router0:

Enable

Configure terminal

Interface fastethernet 0/0

Ip address 192.168.1.1 255.255.255.0

No shutdown

Exit

Interface serial 0/0/0

Ip address 192.168.3.1 255.255.255.0

No shutdown

Clock rate 64000

Exit

Ip route 192.168.2.0 255.255.255.0 serial 0/0/0

CLI commands for Router1:

Enable

Configure terminal

Interface fastethernet 0/0

Ip address 192.168.2.1 255.255.255.0

No shutdown

Exit

Interface serial 0/0/0

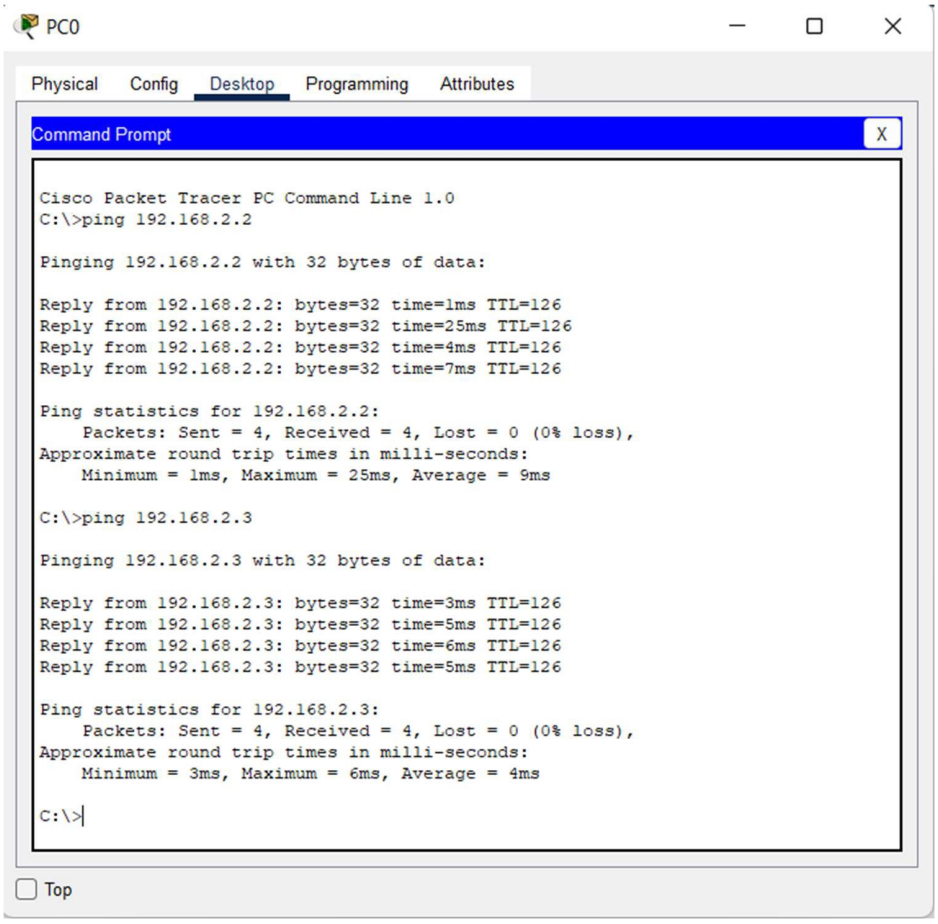
Ip address 192.168.4.1 255.255.255.0

No shutdown

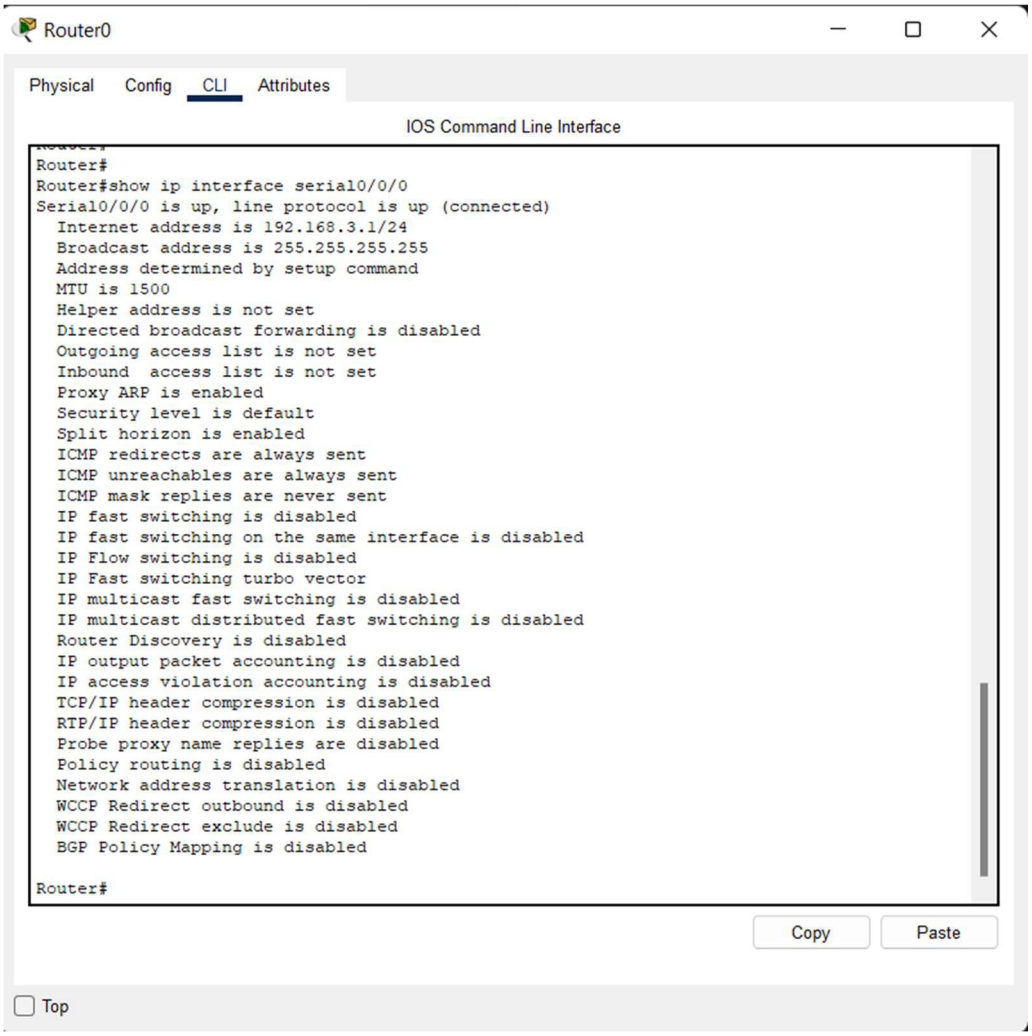
Exit

Ip route 192.168.1.0 255.255.255.0 serial 0/0/0

Ping:


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=25ms TTL=126
Reply from 192.168.2.2: bytes=32 time=4ms TTL=126
Reply from 192.168.2.2: bytes=32 time=7ms TTL=126
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 25ms, Average = 9ms
C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=5ms TTL=126
Reply from 192.168.2.3: bytes=32 time=6ms TTL=126
Reply from 192.168.2.3: bytes=32 time=5ms TTL=126
Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 6ms, Average = 4ms
C:\>
Top

Show ip interface serial 0/0/0:



Encapsulation to PPP:

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial0/0/0
Router(config-if)#encap
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
up
```

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RaOne
RaOne(config)#enable password karuna
RaOne(config)#interface serial0/0/0
RaOne(config-if)#ppp authentication pap
RaOne(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
down
```

Result: IP routing was successfully configured and studied using routing information protocol.

Mini Project No.-8

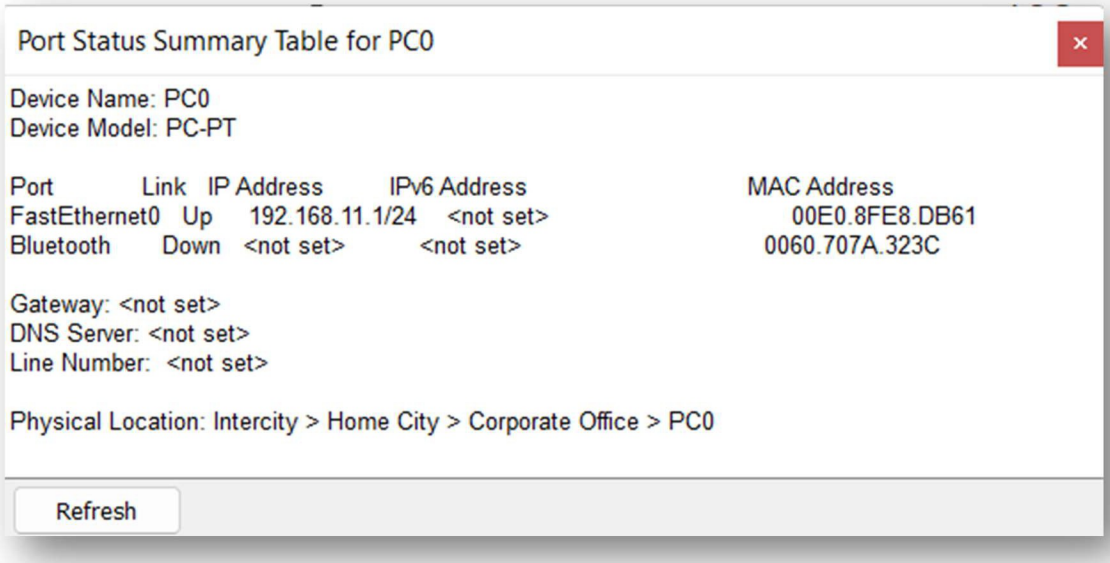
Aim: Simulation of Address Resolution Protocol and Reverse Address Resolution Protocol.

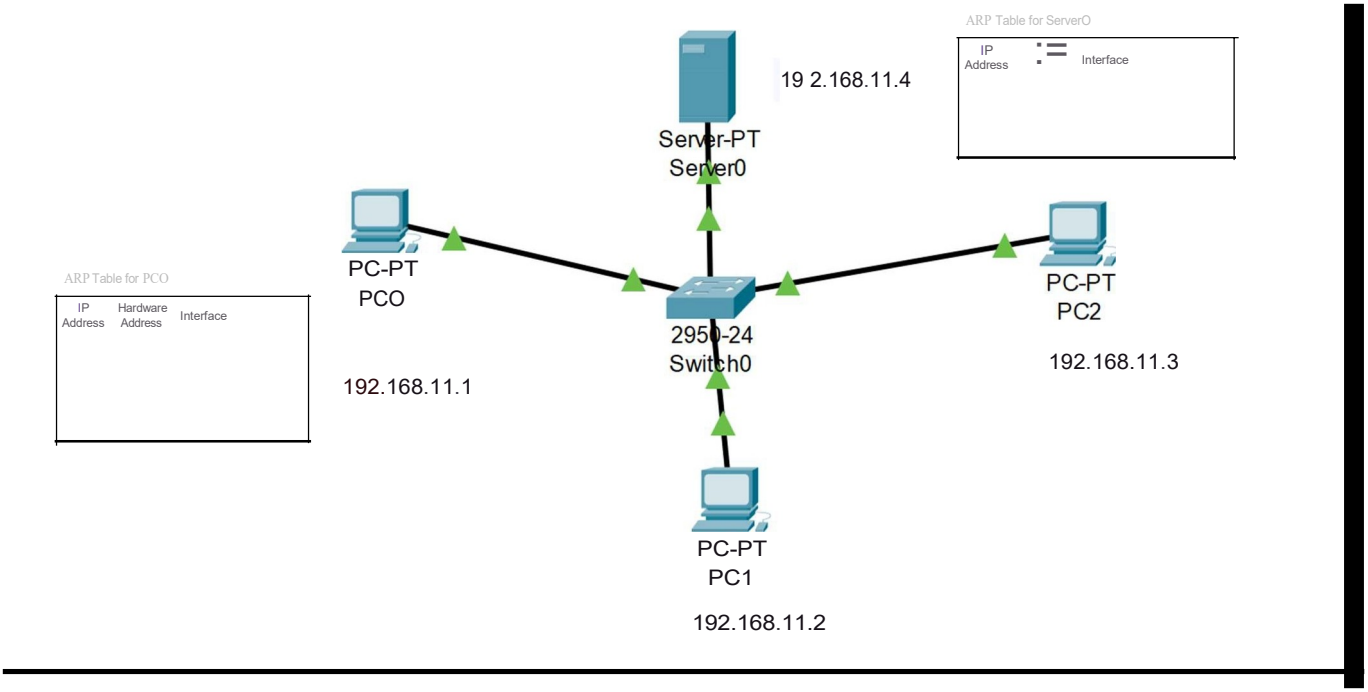
Apparatus: Laptop, Cisco Packet Tracer.

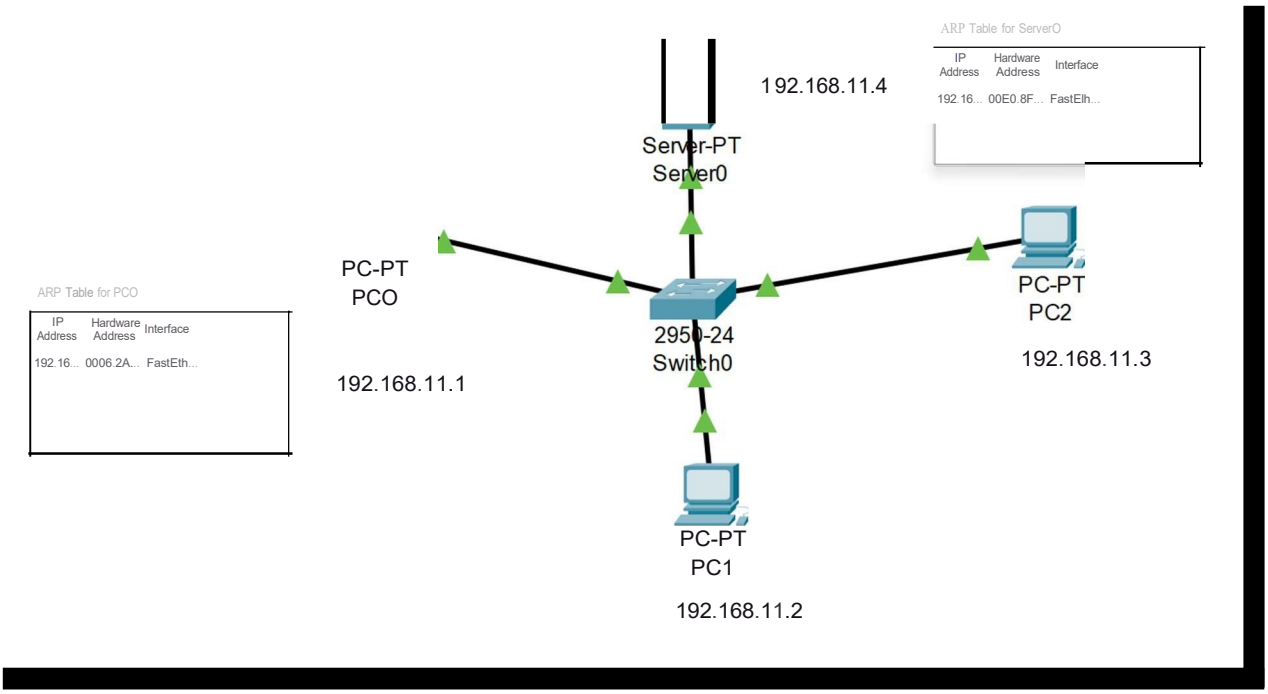
Experiment:

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network LAN. The physical machine address is also known as a media access control (MAC) address. The job of ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice versa. This is necessary because IP addresses in IP version 4 (IPv4) are 32 bits, but MAC addresses are 48 bits.

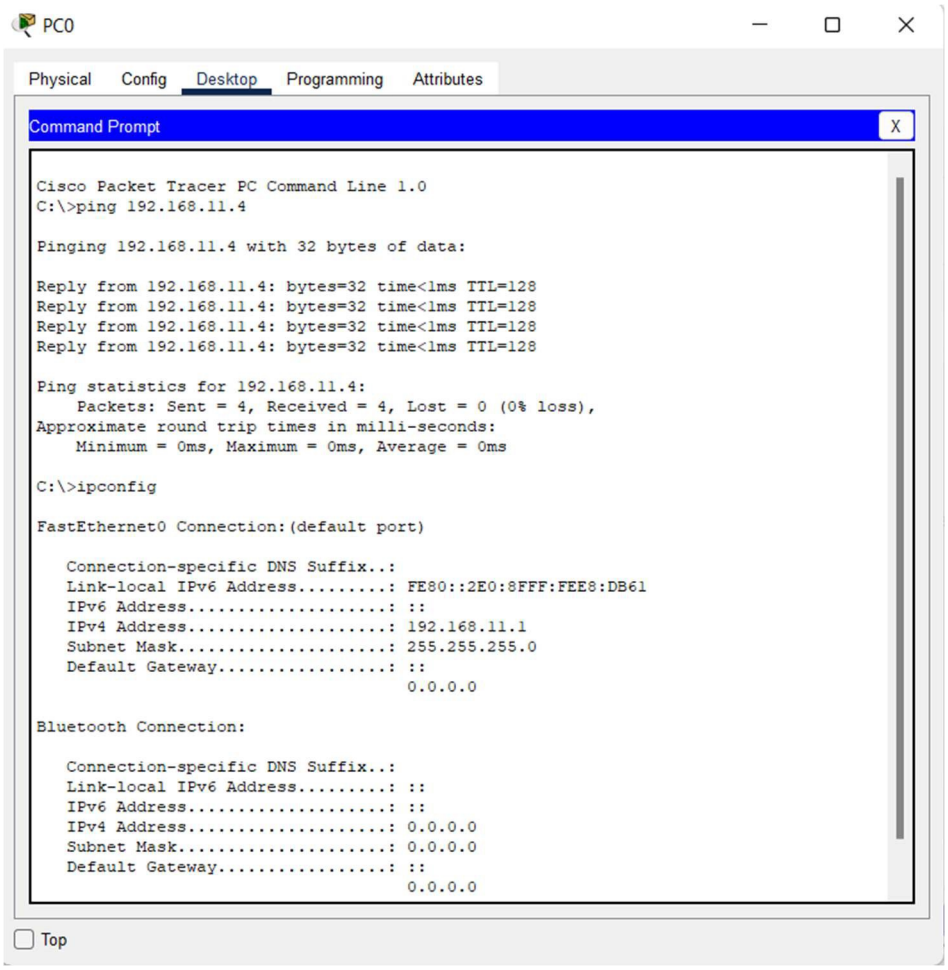
The Reverse Address Resolution Protocol (RARP) is an obsolete computer communication used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address. The client broadcasts the request and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.




ARP Table for ServerO
IP Address
Interface
19 2.168.11.4
Server-PT
Server0
PC-PT
PCO
ARP Table for PCO
IP Address
Hardware Address
Interface
192.168.11.1
2950-24
Switch0
PC-PT
PC2
192.168.11.3
PC-PT
PC1
192.168.11.2


ARP Table for ServerO
IP Address
Hardware Address
Interface
192.16...
00E0.8F...
FastElh...
192.168.11.4
Server-PT
Server0
PC-PT
PCO
ARP Table for PCO
IP Address
Hardware Address
Interface
192.16...
0006.2A...
FastEth...
192.168.11.1
2950-24
Switch0
PC-PT
PC2
192.168.11.3
PC-PT
PC1
192.168.11.2

Ping:



Result: Simulation of Address Resolution Protocol and Reverse Address Resolution Protocol was done and studied.

Mini Project No.-9

Aim: Generation of network traffic in simulation mode and view multiplexing.

Apparatus: Laptop, Cisco Packet Tracer.

Experiment:

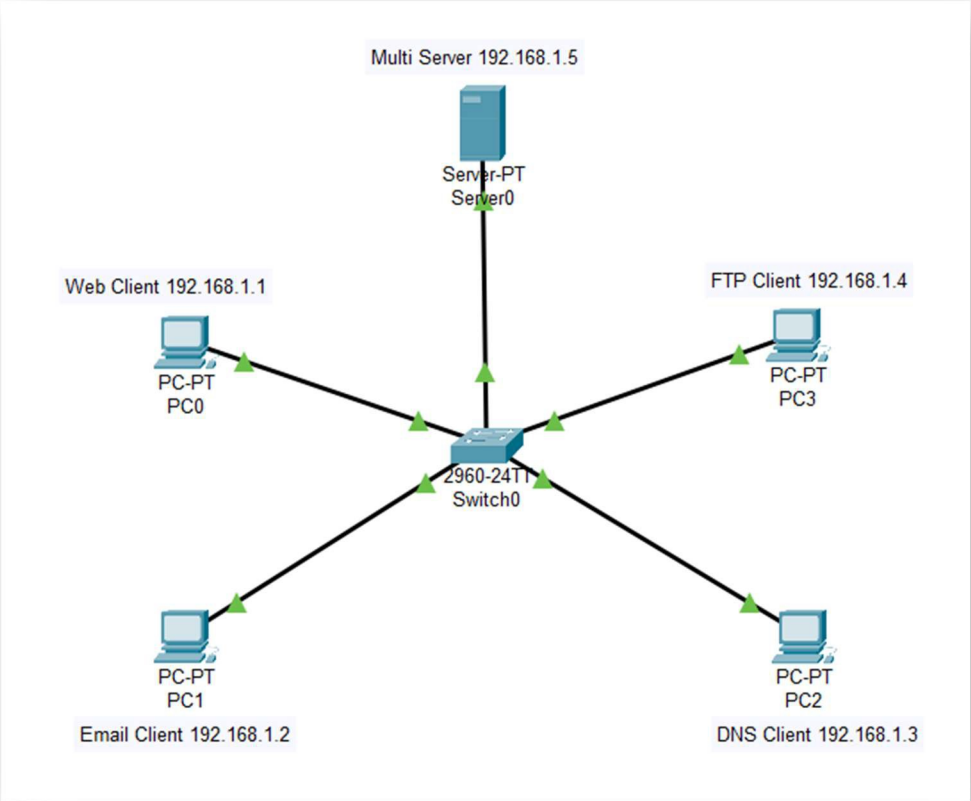
TCP:

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between the different devices over a network.

UDP:

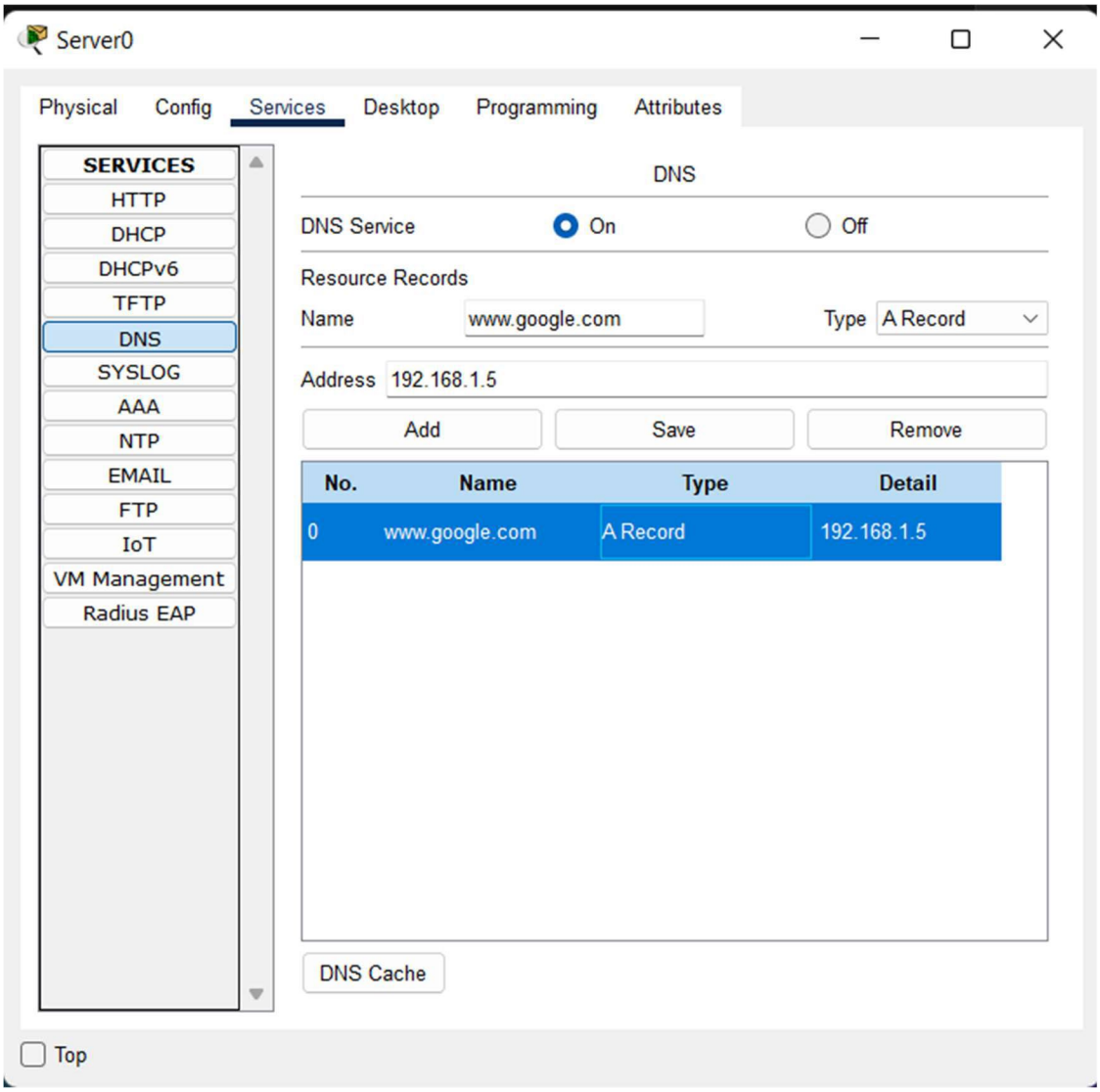
User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection prior to data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process to process communication.

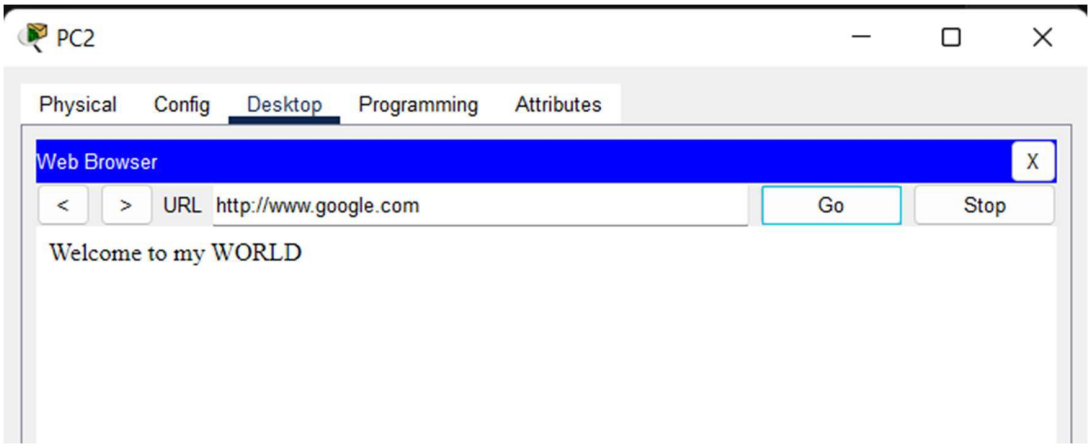
Diagram:



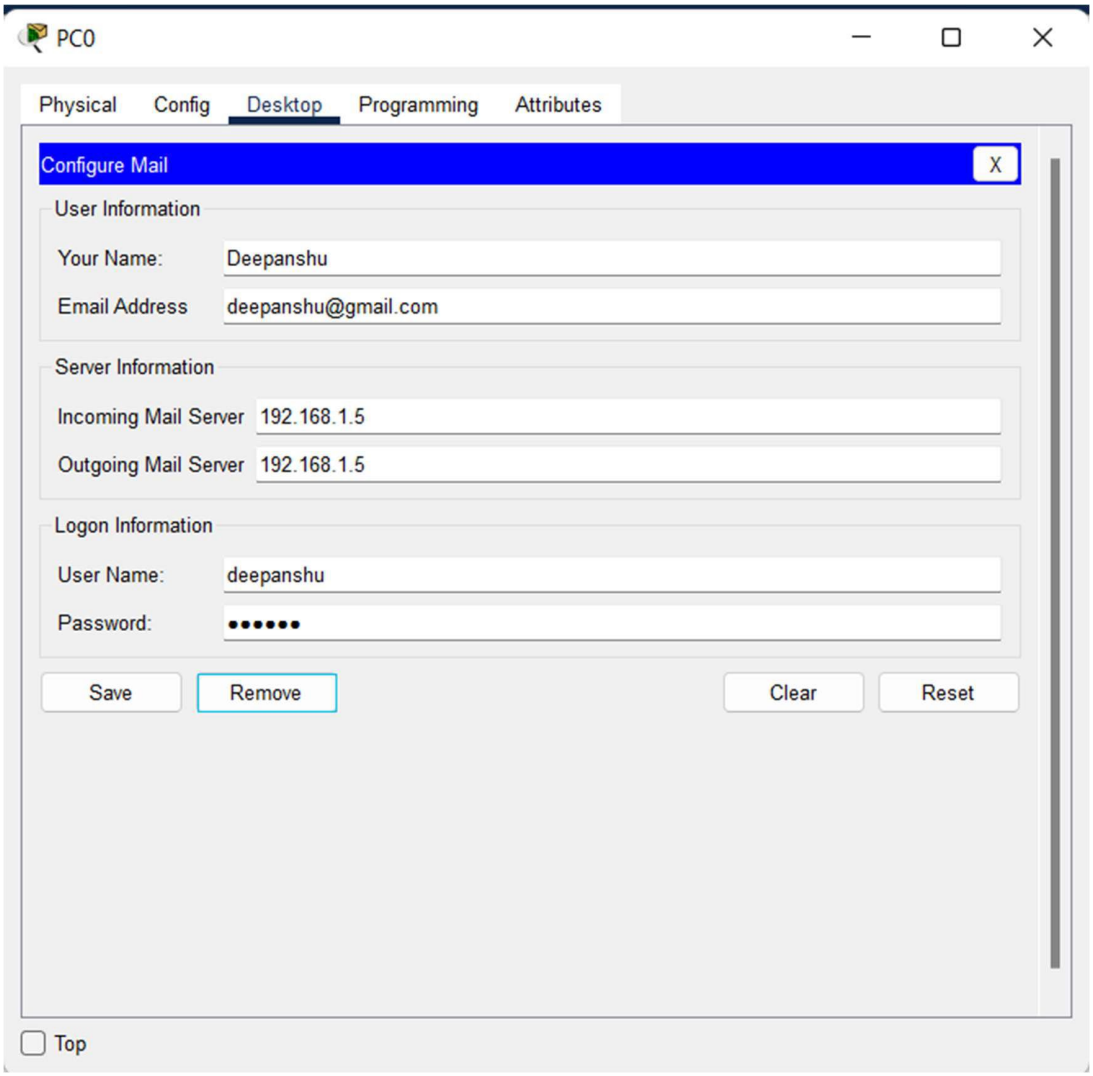
DNS server for all PC's and multi-server: 192.168.1.5

Setting DNS:

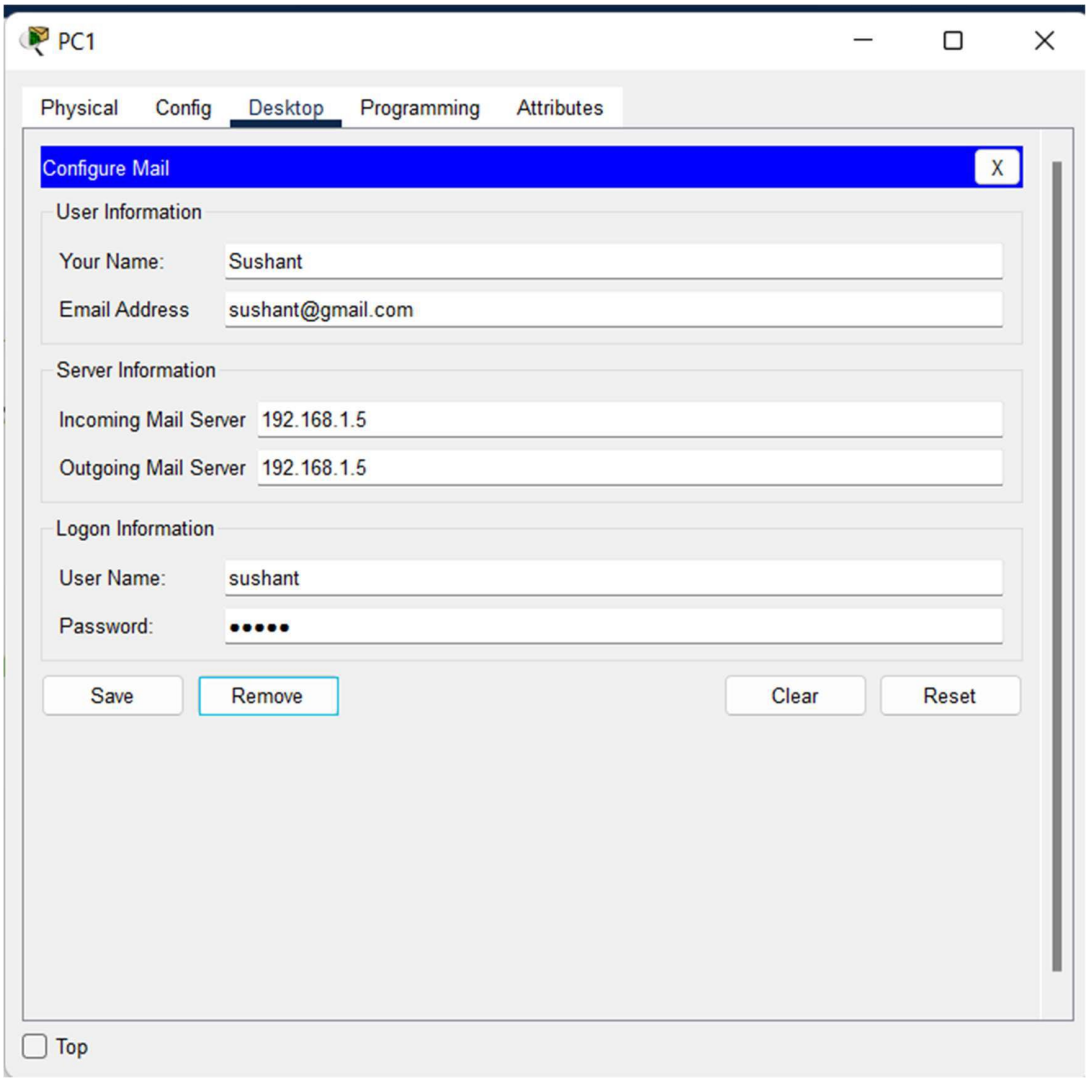

Server0
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DNS
DNS Service
On
Off
Resource Records
Name
www.google.com
Type
A Record
Address
192.168.1.5
Add
Save
Remove
No.
Name
Type
Detail
0
www.google.com
A Record
192.168.1.5
DNS Cache
Top


PC2
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://www.google.com
Go
Stop
Welcome to my WORLD

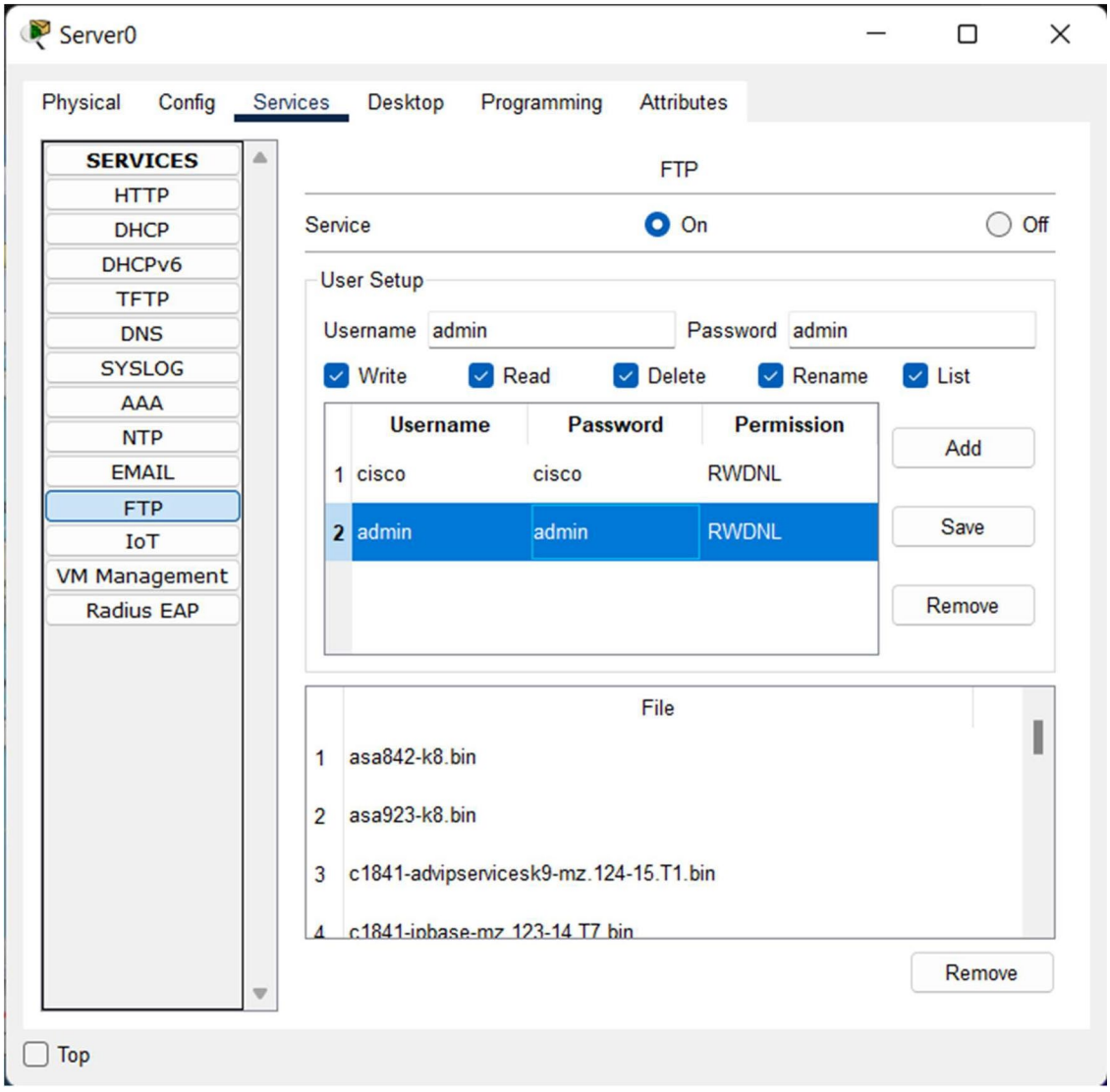
Configuring Mail of Web Client:



Configuring Mail of Email Client:



FTP configuration in Multi Server:



Result: Network traffic in simulation mode is successfully generated with multiplexing.