ERODE SENGUNTHAR
ENGINEERING COLLEGE

(APPROVED BY AICTE, NEW DELHI & PERMANENTLY AFFILIATED TO ANNA UNIVERSITY, CHENNAI
ACCREDITED BY NBA, NEW DELHI, NAAC WITH GRADE "A" & IE(I), KOLKATA)

PERUNDURAI, ERODE - 638 057.

An Autonomous Institution

BONAFIDE CERTIFICATE

Register No. .....

Certified that this is the Bonafide Record of Work Done

Name of the Student :_____

Branch :_____

Name of the Lab :_____

_____

Faculty Incharge

Head of the Department

Submitted for the End Semester Practical

held on.....

Internal Examiner

External Examiner

S.NO	DATE	TITLE OF THE PROGRAM	MARKS	SIGN
1		A Study on Network Topologies		
2		A Study on Cables		
3(a)		Basic Switch Setup		
3(b)		Basic Switch Configuration		
4		VLAN and VTP Configuration		
5		Basic Router Setup		
6		Prepare the Network and Perform all The Necessary Basic Configuration for the Device		
7		Router Serial Interface Configuration		
8		Configure the DHCP Configurations in the Respective		
9		Configure The Port Security For The Ports Connected To The Switches		
10		Configure The Access List in Routers		
11		Verify Connectivity of Directly Connected Networks		
12		Configure RIP Routing on The Router and Verify The Date Configuration and Connectivity		
13		Configure a Network Topology		

Ex. No : 1 **A Study on Network Topologies**

Date :

Aim :

To create various Network Topologies emulated in Packet Tracer 7.3.1.

Topologies:

Network topology is the layout pattern of interconnections of the various elements (links, nodes, etc.) of a computer network.

There are also three basic categories of network topologies:

1. Physical topologies
2. Signal topologies
3. Logical topologies

1. Physical topologies

The mapping of the nodes of a network and the physical connections between them – i.e.,the layout of wiring, cables, the locations of nodes, and the interconnections between the nodes and the cabling or wiring system

Classification of physical topologies

The study of network topology recognizes seven basic topologies:

a) Single Node Topology or Point to Point topology
b) Bus topology
c) Star topology
d) Ring topology
e) Tree topology
f) Mesh topology
g) Hybrid topology

a) Single Node Topology or Point to Point topology: The simplest topology is apermanent link between two endpoints. Switched point-to-point topologies are the basic model of conventional telephony.

Permanent (dedicated)

Point-to-point topology is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints. Children's "tin- can telephone" is one example.

Switched:

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically, and dropped when no longer needed. This is the basic mode of conventional telephony.

b) **Bus topology:** In local area networks where bus topology is used, each machine is connected to a single cable. Each computer or server is connected to the single bus cablethrough some kind of connector. A terminator is required at each end of the bus cable toprevent the signal from bouncing back and forth on the bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it findsthe MAC address or IP address on the network that is the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data.

Alternatively, if the data does match the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable breaks, theentire network will be down.

Advantages of a Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Bus Topology

- Entire network shuts down if there is a break in the maincable.
- Terminators are required at both ends of the backbonecable.
- Difficult to identify the problem if the entire network shutsdown.
- Not meant to be used as a stand-alone solution in a largebuilding.

c) **Star topology:** In local area networks with a star topology, each network host is connected to a central hub. In contrast to the bus topology, the star topology connects each node to the hub with a point-to-point connection. All traffic that traverses the network passes through the central hub. The hub acts as a signal booster or repeater.

Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the hubs,etc.

d) Tree or Expanded Star: A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstationsconnected to a linear bus backbone cable. Tree topologies allow for the expansionof an existing network, and enable schools to configure a network to meet their needs.

Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

e) Ring topology: In local area networks where the ring topology is used, each computer is connected to the network in a closed loop or ring. Each machine or computer has a unique address that is used for identification purposes. The signal passes through each machine or computer connected to the ring in one direction. Ring topologies typically utilize a token passing scheme, used to control access to the network. By utilizing this scheme, only one machine can transmit on the network at a time. The machines or computers connected to the ring act as signal boosters or repeaters which strengthen the signals that traverse the network. The primary disadvantage of ring topology is the failureof one machine will cause the entire network to fail.

f) Mesh topology: The value of fully meshed networks is proportional to the exponent ofthe number of subscribers, assuming that communicating groups of any two endpoints, upto and including all the endpoints, is approximated by Reed's Law

g)Hybrids topology: Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network, but two star networks connected together exhibit a hybrid network topology. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: star ring network and star bus network

2) Signal topology

The mapping of the actual connections between the nodes of a network, as evidenced by the path

that the signals take when propagating between the nodes. The term 'signal topology' is often used synonymously with the term 'logical topology'. By definition, the term 'logical topology' refers to the apparent path that the data takes between nodes in a network while the term 'signal topology' generally refers to the actual path that the signals(e.g., optical, electrical, electromagnetic, etc.) take when propagating between nodes.

3) Logical topology

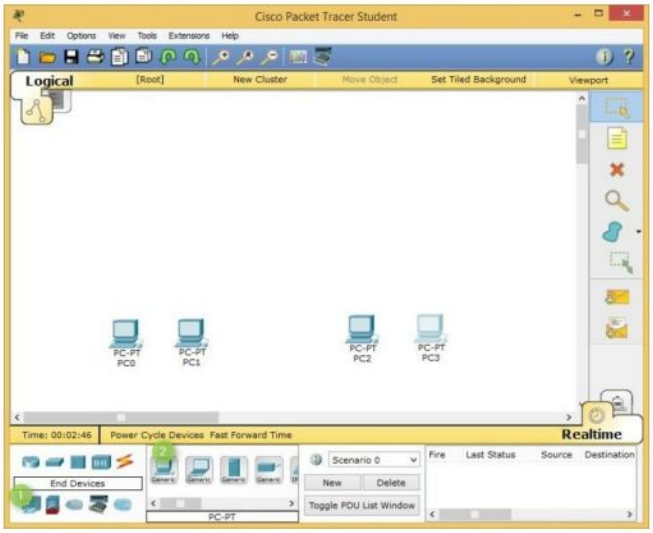
The logical topology, in contrast to the "physical", is the way that the signals act on the network media, or the way that the data passes through the network from one device tothe next without regard to the physical interconnection of the devices. A network's logicaltopology is not necessarily the same as its physical topology.

Procedure:

(i) Adding PCs in Cisco Packet Tracer

To add PCs in Cisco Packet Tracer, you need to perform the following steps:

1. In the Cisco Packet Tracer console, click on the **PC** icon, click **Generic**, and then click in the logical view area to add a **Generic** PC.
2. Repeat the same step to add three more Generic PCs in the logical view area, as shown in the following figure.



(ii) Adding Switches in Cisco Packet Tracer

1. To add a switch in Cisco Packet Tracer, click the **Switch** icon, select a switch type, such as **2960**, and then add the selected switch in the logical view area.
2. Repeat the same step to add one more switch.

(iii) Adding Routers in Cisco Packet Tracer

1. To add a router in Cisco Packet Tracer, click the **Router** icon, select a router type, such as **2811**, and then add the selected router in the logical view area.
2. Repeat the same step to add one more router.

(iv) Understanding Connection Types in Cisco Packet Tracer

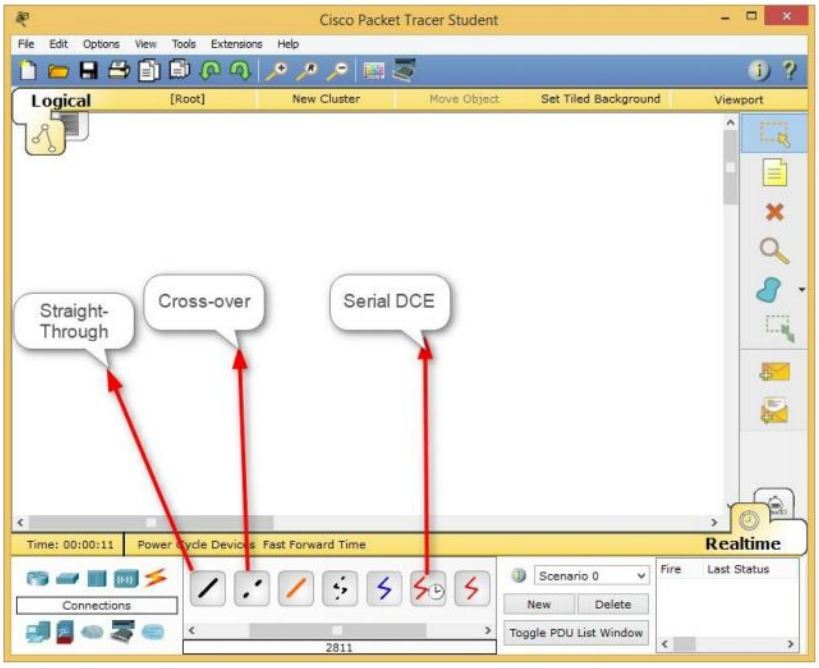
To connect devices in Cisco Packet Tracer, first, you need to understand the various types of cables (connections) used to connect network devices. Some of the common types of cables are:

Straight-through: Used to connect different types of devices (devices that use different wiring standards) such as Router-to-Switch and Switch-to-PC.

1. **Cross-over**: Used to connect same types of devices, such as router-to-router, PC-to-PC, and switch-to-switch.
2. **Serial DCE**: Used to connect router-to-router in a WAN network.
3. **Console**: Used to take console (using hyper terminal) of a router on a PC.

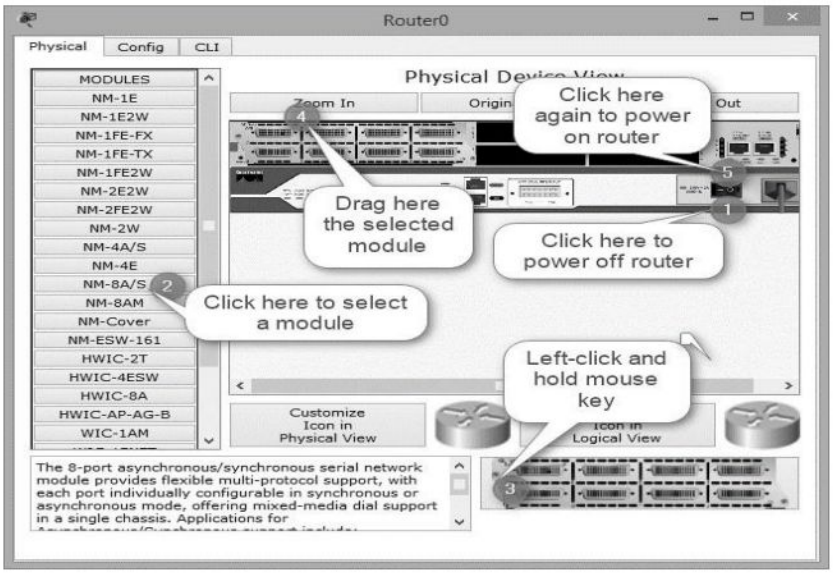
To see the various types of connections, click the **Connection** icon. Spend some time to understand the connections. Once you are familiar with the types of connections, connect the devices to create the network topology.

The following figure displays the various types of connections used to connect devices.



Since we have chosen the modular router (that allows you to modify the number of interfaces), you may need to customize the interfaces before it can be used to connect other network devices. To do this, double-click **Router0**, on the **Router0** properties dialog box, click the **Power** button to power off **Router0**.

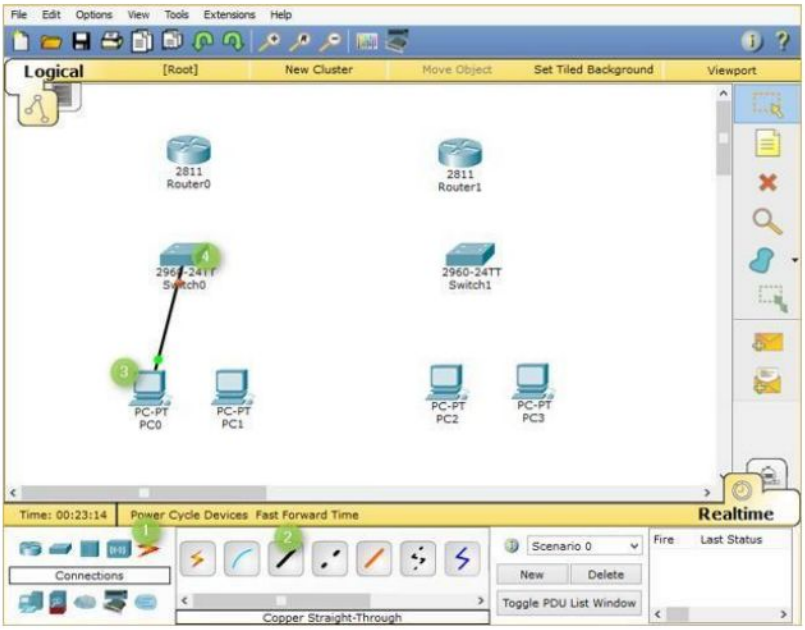
The following figure displays how to add a module in a router using Cisco Packet Tracer.



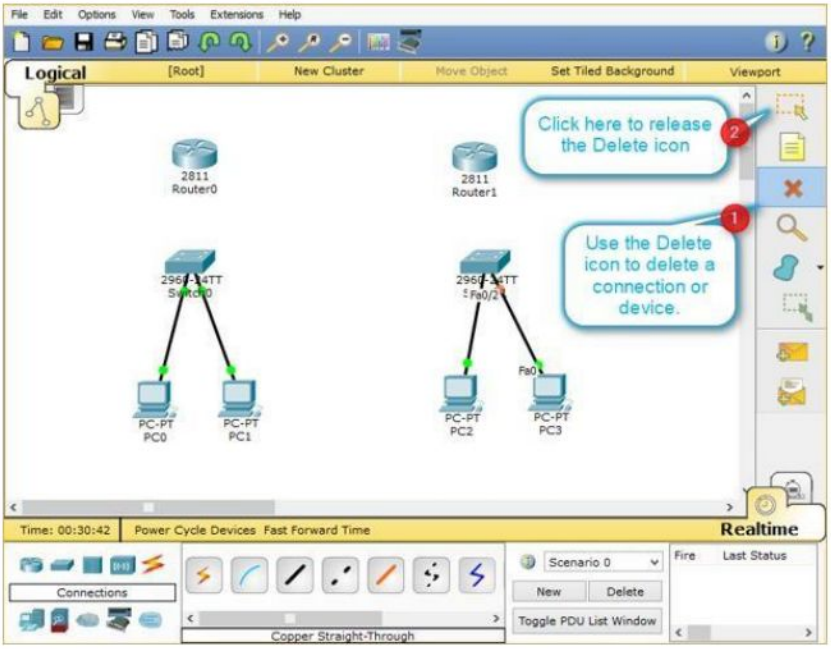
Now, open the **Router1** properties dialog box, add the same module to **Router1** also, and then close the **Router1** properties dialog box.

(V) Connecting Devices in Cisco Packet Tracer

1. To connect devices in Cisco Packet Tracer, click the connection type icon, and selec an appropriate cable. For example, to connect **PC0** to **Switch0**, select the straight-through cable, click on **PC0**, select the **FastEthernet0** interface.
2. Next, click on **Switch0**, and then select the **FastEthernet0/1** interface. The following figure displays how to connect a PC to a switch in Cisco Packet Tracer.



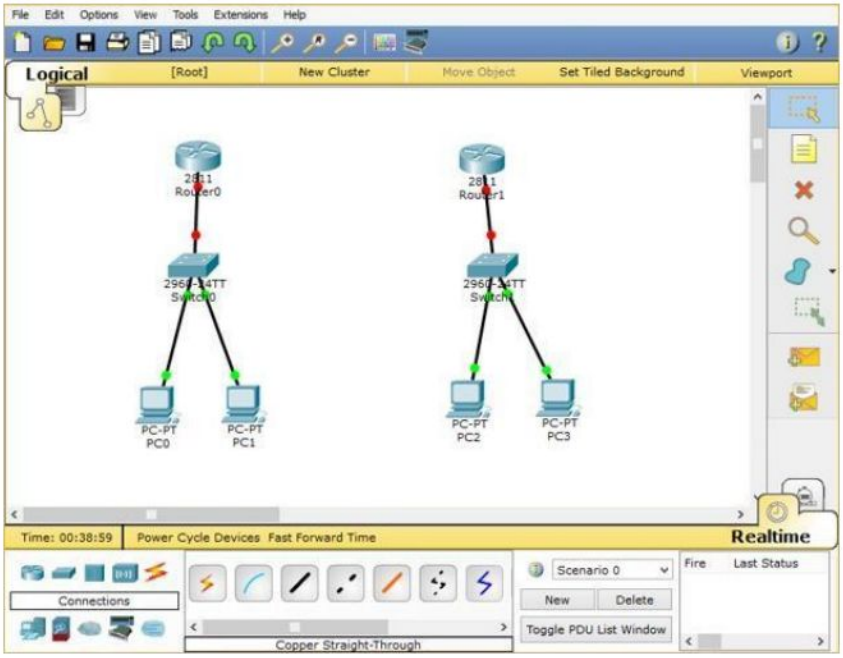
3. Now, add **PC1** to **Switch0** using the **FastEthernet0/2** interface. Also, add **PC2** and **PC3** to the **FastEthernet0/1** and **FastEthernet0/2** interfaces of **Switch1,** respectively.
4. If you have connected a wrong device to a wrong interface, you can use the **Delete** option to delete a connection or device. The following figure displays how to use the **Delete** option to delete a device or connection in Cisco Packet Tracer.



5. Once, you have connected all the PCs to switches, now connect **Switch0** to **Router0,** and **Switch1** to **Router1** using the straight-through cables.

6. Select the straight-through cable, click on **Switch0**, and then select **FastEthernet0/3** interface.
7. Click **Router0** and select the **FastEthernet0/0** interface.
8. Select again the straight-through cable, click on **Switch1**, and select **FastEthernet0/3** interface.
9. Next, click **Router1** and then select the **FastEthernet0/0** interface.

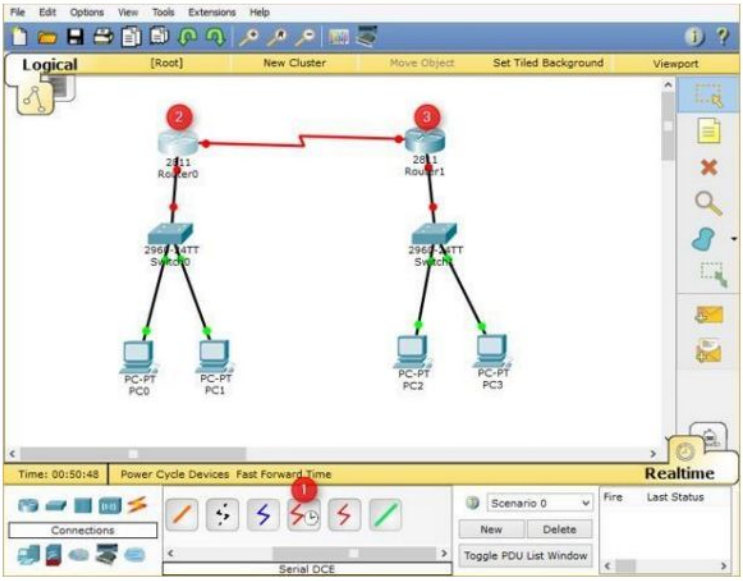
The following figure displays how to connect routers to switches to create a network topology.



(Vi) Interconnecting Routers in Cisco Packet Tracer

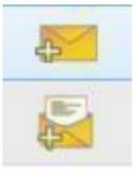
Now, connect **Router0** to **Router1** using the serial connection. To do this, you need to perform the following steps:

1. Select the **Serial DCE** cable, click on **Router0,** and select the **Serial1/0** interface.
2. Click on **Router1** and select the **Serial1/0** interface, as shown in the following figure.

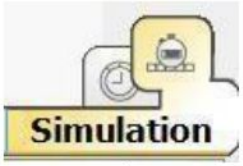


(Vi) Message Transmission

1. In Cisco Packet Tracer, click **File**, and select **Save As**.
2. In the **File name** text box, type a name of the topology, and then click **Save**.
    1. Select “Add simple PDU”.

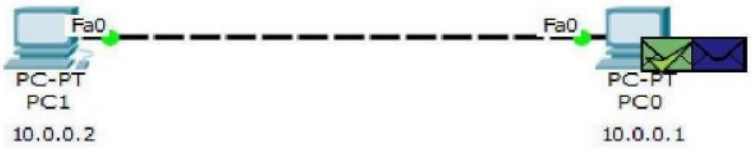


    2. Drag and Drop the message to the source device and then to the Destination device.In this case my source device is PC0 and destination device is PC1.
    3. Select the Simulation Mode at the bottom right corner.

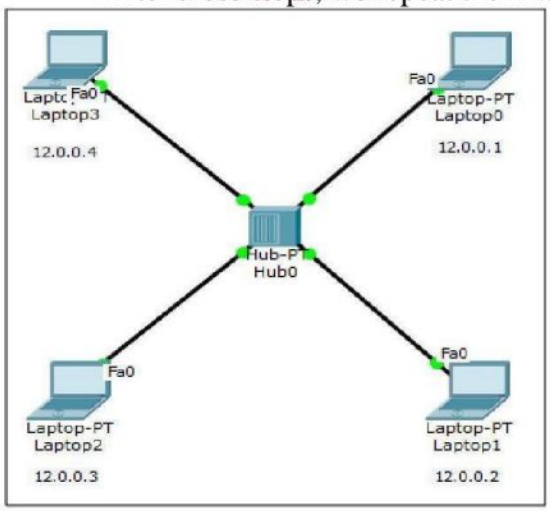


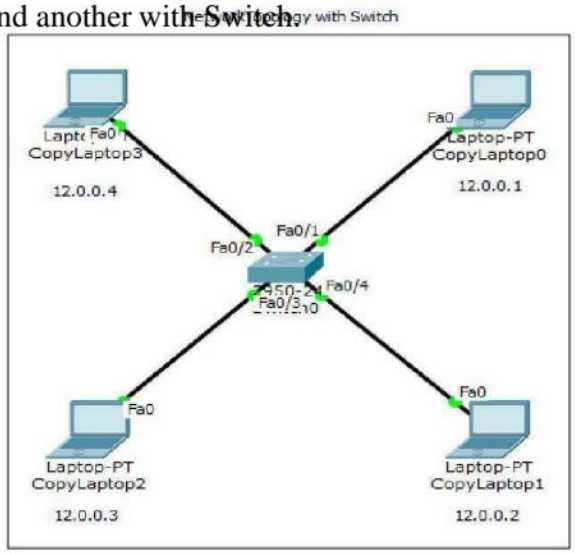
    4. Click at “Auto Capture / Play”.
    5. Observe the path of the Message from source to destination, and back from the destination to the source.

6. Finally observe the marks. If the source PC is marked correct it means youhave successfully established the connection.



- After these steps, we repeat them with Hub and another with Switch.

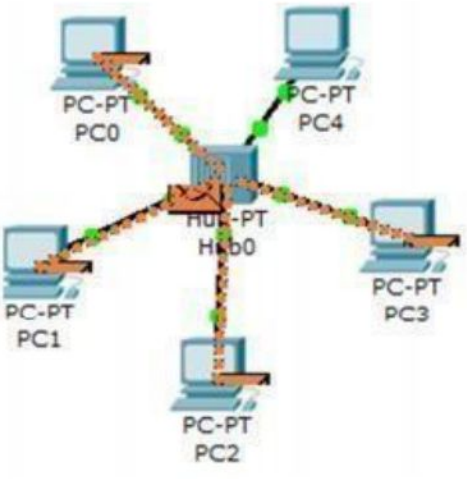


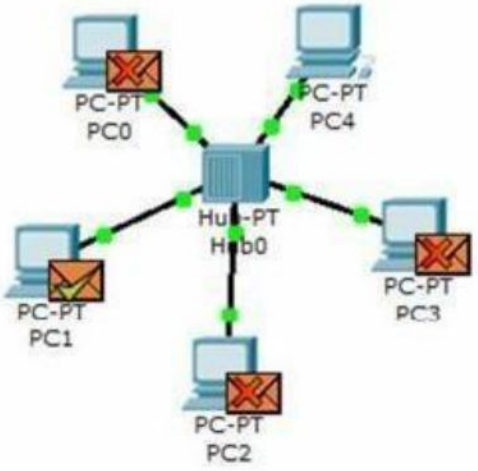


Discussion:

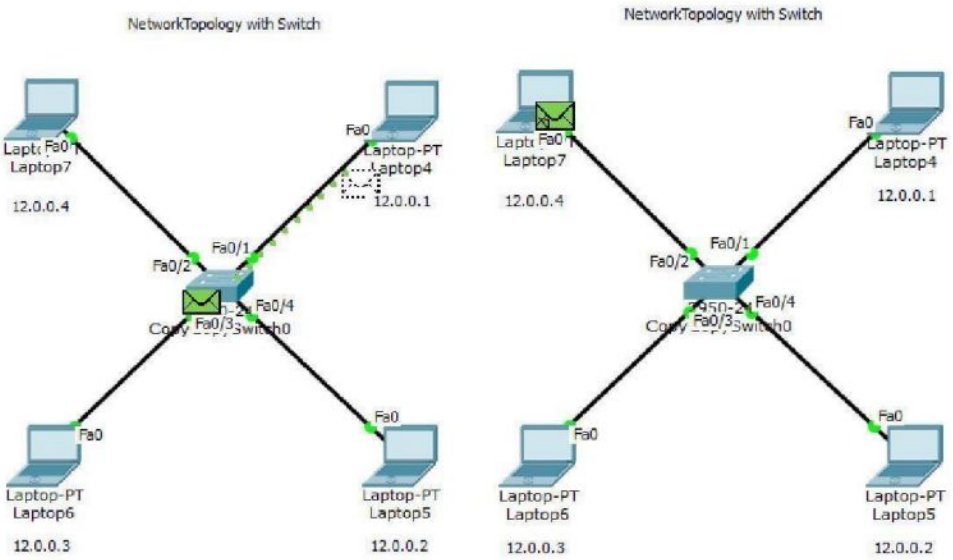
When we use Hub and try to send a simple PDU from a source device to a destination device,the path of the Message was from source to Hub, then to all devices. And then from Destination to Hub then back to the source with the same procedure.

The Switch was the same at the first, but it has a learning attribute that let it build a table contains of MAC address and IP address for each end device that connect to it, so after the first message between two devices, it doesn't send the message to all devices, but to the destination device directly. And this was the result for our test for the Hub: (from PC4 to PC1)





At the first the Switch behave the same, then it send the message directly to the destination, This was our test for Switch: (from PC7 to PC4)



Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

Thus the various network topologies are performed successfully using cisco packet tracer.

Ex. No : 2 **A Study on Cables**

Date :

Aim :

To study various types of Network cables and practically implement the cross-wired cable and straight through cable using clamping tool.

Types of Cables :

To transmit the data the medium must exist, usually in the form of cables or wireless media. Here are some most commonly used cable types.

(i) Thick Coaxial Cables (thick net) (RG-11)

Thick coaxial cables or thick wire is known as the Ethernet standard RG-11. This cable is mostly used as backbone cable, distributing Ethernet signal throughout a building, an office complex or other large installation. It is used in 10base5 Ethernet standard. The length may be up to 500 meters with a max of five segments connected by repeaters. This gives a total distance of 2500 meters.This is called a network diameter. RG-11 cable is typically orange; with black rings around the cable every 2.5-meter to allow taps into the cable.

Thin coaxial cables (thin net) (RG-58)

RG-58 is typically used for wiring laboratories and offices, or another small group of computers. The maximum length of thin wire Ethernet segment is 185 meters, which is due to the nature of the CSMA/CD method of operation, the cable attenuation, and the speed at which signals propagate inside the coax.

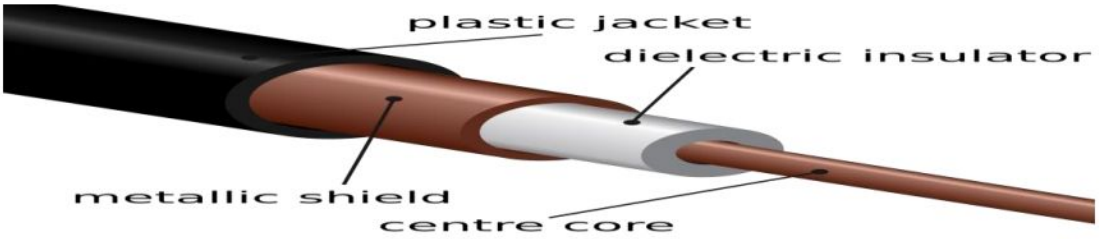


Fig: Thin coaxial cables (thin net) (RG-58)

The length is limited to guarantee that collision is detected when machines that are apart transmit at the same time. BNC connectors are used to terminate each end of the cable. When many machines are connected to the same Ethernet segment, a daisy chain approach is used. The BNC connectors allow the networkinterface card to the next machine. The machine each end of the cable must use aterminating resistor to eliminate collision-causing reflection in the cable.

Coaxial Cable Connectors

Coaxial connectors are needed to connect coaxial cable to devices. The most common type of connector used today is the Bayone-Neil-Concelman, in short, BNC connector.

Coaxial Cable Connector

The three popular types of connectors are: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device.

The BNC terminator is used at the end of the cable to prevent the reflection ofthe signal.

Applications

1. Coaxial cable was widely used in analog telephone networks, and later with digital telephone networks.
2. Cable TV networks use coaxial cables (RG-59) at the network boundaries. However, coaxial cable has largely been replaced today with fiber-optic cable due to its higher attenuation.
3. Traditional Ethernet LAN
   – 10Base-2, or thin Ethernet, uses RG-58 coax cable with BNCconnectors.
   – 10Base-5, or thick Ethernet, uses RG-11 coax cable with specialized connectors.

Twisted pair cables

Twisted pair is probably the most widely used cabling system in Ethernet in networks. Two copper wires twist around each other to form the twisted pair cable. Depending on category several insulated wire strands can reside in the cable.

Twisted pair is available in two basic types

a) Unshielded Twisted Pair (UTP)

b) Shielded Twisted Pair (STP)

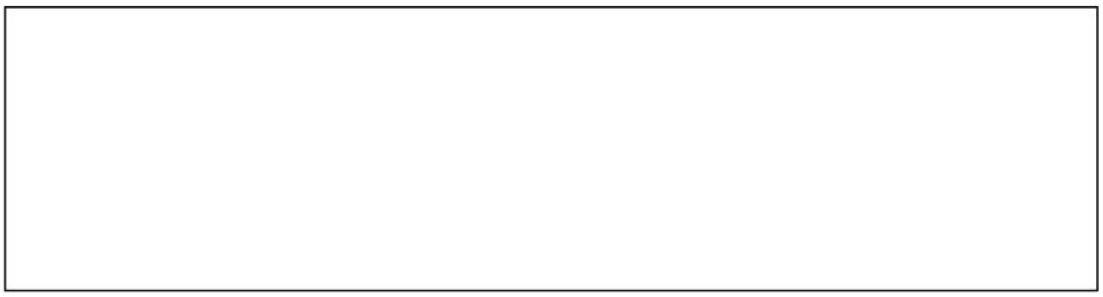


Fig: Twisted pair cables

Unshielded Twisted Pair

Mostly the UTP is used. A twisted pair segment can't exceed 100 meters. This limitation is the only drawback to twisted pair. Twisted pair is used for 10/100 based Ethernet networks. UTP cables are wired as straight through or crossover cables. Straight through cables

typically connect the computer's networks interface can't to be a port on the hub. Crossover cables are used for NIC to communication and for hub-to-hub connections when no crossover port is available.

Category	Descriptor
1	Used for voice for data.
2	Contains four twisted pair and a data transmission up to 4 Mbps. Used for some token ring network.
3	Contains four twisted pair and a data transmission up to 10 Mbps. Used for some token ring network.
4	Contains four twisted pair and a data transmission up to 16 Mbps. Used for some token ring network.
5	Contains four twisted pair and a data transmission up to 100 Mbps. Used for some token ring network.

Category-5 cables can be purchased or crimped as either straight through or crossed. A category-5 cable has 8 thin. Colours coded wires inside that run from one end of the cable to the other. Ethernet networks for communication use only wires 1, 2, 3 and to be connected in both jacks. Straight through cables are used for connecting to a hub. Crossed cables are used for connecting a hub to another hub (there is an exception: some hubs are a built in uplink port that is crossed internally, which allows you to uplink hubs with a straight cable instead.) In a straight through cable wires 1, 2, 3…. and 6 at the other end. In a crossed cable, one order of the wires change from one end to the other wire 1 becomes 3 and 2 becomes 6.

For PC 2 PC Communication without HUB (Cross Cable Connection)

Sl. No.	One Site	Second Site	Pin Configuration
01	Orange White	Green White	Transmit
02	Orange	Green	Transmit
03	Green White	Orange White	Receive
04	Blue	Blue	Not Use
05	Blue White	Blue White	Ground
06	Green	Green	Receive
07	Brown White	Brown White	DTR
08	Brown	Brown	DTS

For PC 2 PC Communication with HUB (Simple Cable Connection)

Sl. No.	One Site	Second Site	Pin Configuration
01	Orange White	Orange White	Transmit
02	Orange	Green	Transmit
03	Green White	Orange White	Receive

04	Blue	Blue	Not Use
05	Blue White	Blue White	Ground
06	Green	Green	Receive
07	Brown White	Brown White	DTR
08	Brown	Brown	DTS

For One Cable in Two PC Communication through HUB (Simple Cable Connection)

First Connection

Sl. No.	One Site	Second Site	Pin Configuration
01	Orange White	Green White	Transmit
02	Orange	Orange	Transmit
03	Green White	Green White	Receive
04	Green	Green	Receive

Second Connection:

Sl. No.	One Site	Second Site	Pin Configuration
01	Blue	Green White	Transmit
02	Blue White	Orange	Transmit
03	Brown White e	Green White	Receive
04	Brown	Green	Receive

Shielded Twisted Pair It is 150Ω cable containing additional shielding that protects signals against electromagnetic Interference (EMI) produced by electric motors power lines etc. It is primarily used in Token Ring Network & where UTP cable would provide insufficient protection against interface. Wires within cables are encased in a metallic sheath that is conductive as copper in wires. Thissheath when properly grounded converts it ambient noise into current, like antenna. This current is carried to wires within where it creates an equal and opposite current flowing in twisted pair thus getting cancelled and no noisesignal is resulted.

Unshielded Twisted-Pair Connector

The most common Unshielded Twisted-Pair connector is RJ45. RJ stands for registered jack.

Inside the Ethernet cable, there are 8 color coded wires, with all eight pins used as conductors. These wires are twisted into 4 pairs and each pair has a common

color theme. RJ45 specifies the physical male and female connectors as well as the pin assignments of the wires.

RJ45 uses 8P8C modular connector, which stands for 8 Position 8 Contact. It is akeyed connector which means that the connector can be inserted only in a single way. RJ45 is used almost exclusively to refer to Ethernet-type computer connectors.

Characteristics of twisted pair cable

1. Requires amplifiers every 5-6 km foranalog signals
2. Requires repeaters every 2-3 km fordigital signals
3. Attenuation is a strong function offrequency
4. Susceptible to interference and noise

Applications

1. Used in telephone lines to provide
   voice and data channels.
2. The local loop –the line connecting the subscriber to the central telephone office- commonly consists of UTP cables.
3. DSL lines are also UTP cables.
4. LANs such as, 10Base-T and 100Base-T use UTP cables.

Fibre Optic.

Fibre Optic relies on pulsed as light to carry information. Two types of plastic or glass with different physical properties are used (the inner core and the outer cladding) to allow a beam of light to reflect off the boundary between the core and cladding. Some fibre optic cables allow many different paths other allow onesingle mode. They are called multimode and single mode fibres. A popular multimode fibre has core/cladding dimensions of 62.5/125 nanometres.

Fiber Optic cable connector

Diagram shows you how to prepare Cross wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Diagram shows you how to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result:

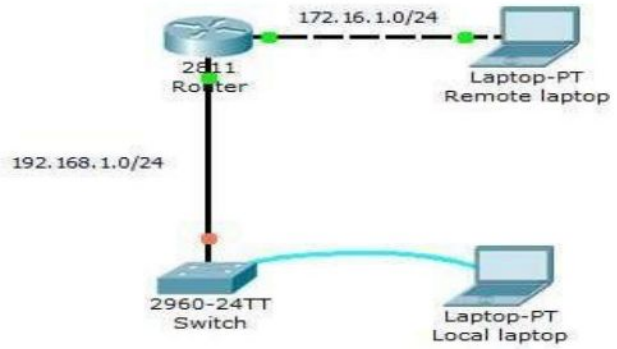
Thus various types of cables are studied

Ex. No : 3 a **Basic switch setup**

Date :

Aim :

To configure basic settings such as hostname, motd banner, encrypted passwords, and terminal options ona Cisco Catalyst 2960 switch emulated in Packet Tracer 7.3.1.



1. Use the local laptop connect to the switch console and configure the laptop with the right parameters forconsole access to the Cisco 2960 Catalyst switch

2. Configure Switch hostname as LOCAL-SWITCH

3. Configure the message of the day as "Unauthorized access is forbidden"

4. Configure the password for privileged mode access as "cisco". The password must be md5 encrypted

5. Configure password encryption on the switch using the global configuration command

6. Configure CONSOLE access with the following settings :
- Login enabled
- Password : ciscoconsole
- History size : 15 commands
- Timeout : 6'45"
- Synchronous logging

7. Configure TELNET access with the following settings :
- Login enabled
- Password : ciscotelnet
- History size : 15 commands
- Timeout : 8'20"
- Synchronous logging

8. Configure the IP address of the switch as 192.168.1.2/24 and it's default gateway IP (192.168.1.1).

9. Test telnet connectivity from the Remote Laptop using the telnet client.

Lab solution

Configure Switch hostname as LOCAL-SWITCH

Switch(config)#hostname LOCAL-SWITCH

Configure the message of the day as "Unauthorized access is forbidden"

Switch(config)#banner motd #
Unauthorized access is
forbidden#

Configure the password for privileged mode access as "cisco". The password must be md5 encrypted

Switch(config)#enable secret cisco

Configure password encryption on the switch using the global configuration command

Switch(config)#service password-encryption

Configure CONSOLE access [...]

Switch(config)#line con 0
Switch(config-line)#password
ciscoconsoleSwitch(config-line)#logging
synchronous Switch(config-line)#login
Switch(config-line)#history size 15
Switch(config-line)#exec-timeout 6 45

Configure TELNET access [...]

Switch(config)#line vty 0 15
Switch(config-line)#exec-timeout 8 20
Switch(config-line)#password
ciscotelnetSwitch(config-line)#logging
synchronousSwitch(config-line)#login
Switch(config-line)#history size 15

Configure the IP address of the switch as 192.168.1.2/24 and it's default gateway IP (192.168.1.1).

Switch(config)#interface Vlan1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#ip default-gateway 192.168.1.1

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

Thus the basic switch setup is performed succe ssfully using Cisco packet tracer.

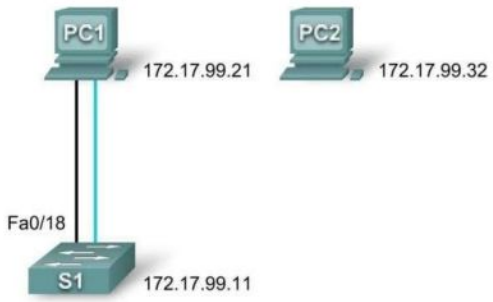
Ex.No. : 3 b **Basic Switch Configuration**

Date :

Aim :

To examine and configure a standalone LAN switch using cisco packet tracer.

Topology :



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	**NIC**	172.17.99.21	255.255.255.0	172.17.99.11
PC2	**NIC**	172.17.99.32	255.255.255.0	172.17.99.11
S1	**VLAN99**	172.17.99.11	255.255.255.0	172.17.99.1

Task 1: Cable, Erase, and Reload the Switch

Step 1: C ble a network.

Cable a network that is similar to the one in the topology diagram. Create a console connectic to the switch.

You can use any current switch in your lab as long as it has the required interfaces shown in the toı ology. The output shown in this lab is from a 2960 switch. If you use other switches, the switch outputs and interface descriptions may appear different.

Note: PC2 is not initially connected to the switch. It is only used in Task 5.

Step 2: C ear the configuration on the switch.

Clear the configuration on the switch using the procedure in Appendix 1.

Task 2: Verify the Default Switch Configuration

Step 1: Enter privileged mode.

You can access all the switch commands in privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. You will set passwords in Task 3.

The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command.
Switch> enable

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2: Examine the current switch configuration.

Switch#**show running-**

configSwitch#**show**

startup-config startup-

config is not present

Examine the characteristics of the virtual interface VLAN1:

Switch#**show interface vlan1**

Switch#**copy running-config startup-config**
Destination filename [startup-config]?

(enter) Building configuration...

[OK]

S1#**show startup-config**

Task 3: Create a Basic Switch Configuration

Step 1: Assign a name to the switch.

S1#**configure terminal**
S1(config)#**hostname S1** S1(config)#**exit**

Step 2: Set the access passwords.

Enter config-line mode for the console. Set the login password to **cisco**. Also configure the vty lines 0 to 15 with the password

cisco.S1#**configure terminal**

Enter the configuration commands, one for each line. When you are finished, return toglobal configuration mode by entering the **exit** command or pressing Ctrl-Z.

S1(config)#**line console 0**
S1(config-line)#**password cisco**

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

Thus the switch is configured successfully using packet tracer.

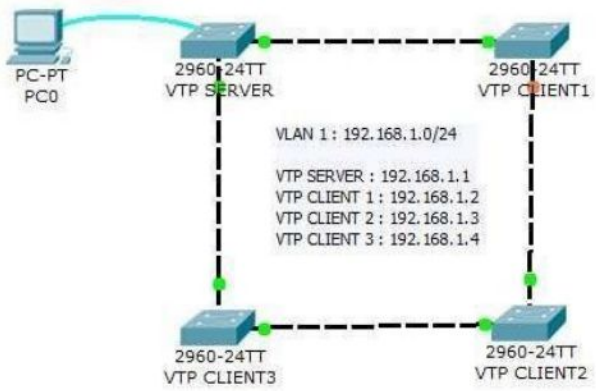
Ex.No. : 4 **VLAN and VTP Configuration**

Date :

Aim :

To configure VLAN and VTP on a small network of 4 switches using Packet Tracer

Network diagram



1. Configure the VTP-SERVER switch as a VTP server

2. Connect to the 3 other switches and configure them as VTP clients.All links between swiches must be configured as trunk lines.

3. Configure VTP domain name as "TESTDOMAIN" and VTP password as "cisco"

4.Configure VLAN 10 with name "STUDENTS" and VLAN 50 with name

"SERVERS"

5. Check propagation on all switches of the VTP domain.

Solution :

1. Configure the VTP-SERVER switch as a VTP serverVTP-SERVER(config)#vtp mode

server

Verify the VTP operating mode using the show vtp status command

VTP-SERVER#show vtp status

VTP Version 2

Configuration Revision 4

Maximum VLANs supported locally 255

Number of existing VLANs 7

VTP Operating Mode : Server

VTP Domain Name : TESTDOMAIN

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0xAE 0x4F 0x3F 0xC5 0xD3 0x41 0x9C

0x11Configuration last modified by 192.168.1.1 at 3 1-93 00:27:41

Local updater ID is 192.168.1.1 on interface Vl1 (lowest numbered VLAN interface found)

2. Connect to the 3 other Catalyst switches and configure them as VTP clients.All links between swiches must be configured as trunk lines.

VTP-CLIENT3(config)#vtp mode

clientVTP-CLIENT3(config)#vtp

mode client

Verify the VTP operating mode of the switch using the show vtp status command.

VTP-CLIENT3#sh vtp status

VTP Version 2

Configuration Revision 4

Maximum VLANs supported locally :

255Number of existing VLANs 7

VTP Operating Mode : Client

VTP Domain Name : TESTDOMAIN

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation :

Disabled

MD5 digest : 0xAE 0x4F 0x3F 0xC5 0xD3 0x41 0x9C

0x11Configuration last modified by 192.168.1.1 at 3-1-93 00:27:41

Configure each link between switches as a trunk line using the switchport mode truink command

#interface GigabitEthernet1/1

#switchport mode trunk

#interface

GigabitEthernet1/2

#switchport mode trunk

3. Configure VTP domain name as "TESTDOMAIN" and VTP password as "cisco"On the VTP

server Catalyst switch:

VTP-SERVER(config)#vtp domain

TESTDOMAINVTP-SERVER(config)#vtp

password cisco

On each VTP client switch :

VTP-CLIENT1(config)#vtp password cisco

VTP-CLIENT1(config)#vtp domain TESTDOMAIN

4. Configure VLAN 10 with name "STUDENTS" and VLAN 50 with name "SERVERS"

On the VTP server Catalyst 2960 switch, configure the following commands to create both "STUDENTS"and "SERVERS" vlans :

5. Check propagation of both "STUDENTS" and "SERVERS" vlans on all Catalyst 2960 network switchesof the VTP domain.

Use the show vlan brief on each switch to check propagation of the 2 VLANS.

VTP-SERVER#show vlan brief

VLAN	Name	Status	Ports
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, [...]
10	STUDENTS	active	
50	SERVERS	active	

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

Thus the VLAN and VTP configuration is successfully performed using Packet tracer.

Ex. No. : 5 **Basic Router setup**

Date:

Aim :

To perform basic configuration to secure administrative access to the router using packet tracer.

Network diagram

The aim of this lab is to test your ability to perform a basic router setup.

1. Configure the LAPTOP terminal software with the right console parameters.

2. Configure the router hostname to "GATEWAY"

3. Configure the enable password and secret to "cisco"

4. Configure password encryption on the router to secure stored passwords

5. Configure the console access :
   - Login : yes
   - Password : "cisco"
   - History : 10 commands
   - Logging synchronous
   - Timeout : 2 minutes 45 seconds.

Solution

1. Configure the laptop terminal software

The terminal software in not correctly configured on the laptop. You have to change the settings to **9600 /8 / None / 1** to connect to the router's console.

2.Configure the router's name

The **hostname** command has to be used to change the router's hostname.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname GATEWAY

4. Configure the enable password and secret to "cisco"

The **enable secret <password>** command stores a MD5 hash of the password required for privileged mode access. The enable secret password of a Cisco ISR router is used for restricting access to enable mode and to the global configuration mode (configure terminal) of a router.

GATEWAY(config)#enable secret cisco

5. Configure password encryption for this router

GATEWAY(config)#service password-encryption

6. Configure the console access

Console access is protected by the 'cisco' password and login is required at console access.

The **exec-timeout** command automatically logs off user from console after defined inactivity period (2'45"in this lab)

GATEWAY(config)#line console 0
GATEWAY(config-line)#password cisco
GATEWAY(config-line)#login
GATEWAY(config-line)#logging
synchronousGATEWAY(config-line)#exec-
timeout 2 45
GATEWAY(config-line)#history size 10

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

Thus the router is configured successfully using Packet tracer.

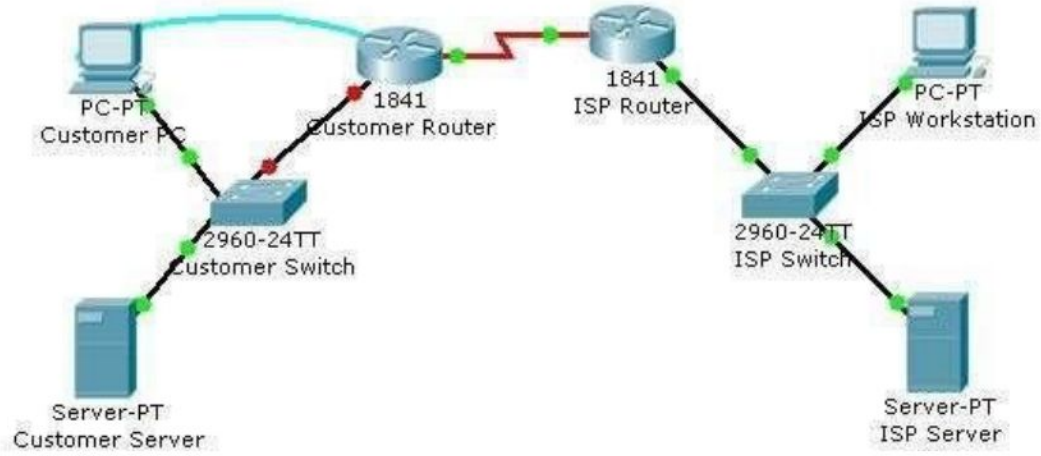
Ex.No. : 6 **Prepare the Network and perform all the necessary basic**

Date : **configurations for the device.**

Aim:

To prepare the network and perform all the necessary basic configurations for the device.

Topology Diagram



Objectives

- Configure the router host name.
- Configure passwords.
- Configure banner messages.
- Verify the router configuration.

Background / Preparation

In this activity, you will use the Cisco IOS CLI to apply an initial configuration to a router, including hostname, passwords, a message-of-the-day (MOTD) banner, and other basic settings.

Note: Some of the steps are not graded by Packet Tracer.

Step 1: Configure the router host name.

- On Customer PC, use the terminal emulation software to connect to the console of the customer Cisco1841 ISR.

Set the host name on the router to **CustomerRouter** by using these commands.

Router>**enable**
Router#**configure terminal**

Router(config)#**hostname CustomerRouter**

Step 2: Configure the privileged mode and secret passwords.

a. In global configuration mode, set the password to cisco.

CustomerRouter(config)**#enable password cisco**

Set an encrypted privileged password to cisco123 using the secret command.

CustomerRouter(config)**#enable secret cisco123**

Step 3: Configure the console password.

a. In global configuration mode, switch to line configuration mode to specify the console line.

CustomerRouter(config)#line console 0

Set the password to cisco123, require that the password be entered at login, and then exit line configuration mode.

CustomerRouter(config-line)#**password cisco123**

CustomerRouter(config-line)#**login**

CustomerRouter(config-line)#**exit**

CustomerRouter(config)#

Step 4: Configure the vty password to allow Telnet access to the router.

a. In global configuration mode, switch to line configuration mode to specify the vtylines.

CustomerRouter(config)#**line vty 0 4**

Set the password to cisco123, require that the password be entered at login, exit line configuration mode, and then exit the configuration session.

CustomerRouter(config-line)#**password cisco123**

CustomerRouter(config-line)#**login**

CustomerRouter(config-line)#**exit**

CustomerRouter(config)#

Step 5: Configure password encryption, a MOTD banner, and turn off domain server lookup.

a. Currently, the line passwords and the enable password are shown in clear text when you show the running configuration. Verify this now by entering the show running-config command.

To avoid the security risk of someone looking over your shoulder and reading the passwords, encrypt all clear text passwords.

CustomerRouter(config)#**service password-encryption**

Use the **show running-config** command again to verify that the passwords are encrypted.

To provide a warning when someone attempts to log in to the router, configure a MOTD banner.

CustomerRouter(config)#**banner motd $Authorized Access Only!$**

Test the banner and passwords. Log out of the router by typing the exit command twice. The banner displays before the prompt for a password. Enter the password to log back into the router.

You may have noticed that when you enter a command incorrectly at the user or privileged EXEC prompt, the router pauses while trying to locate an IP address for the mistyped word you entered. For example, this output shows what happens when the enable command is mistyped.

CustomerRouter>emable

Translating "emable"...domain server (255.255.255.255)

To prevent this from happening, use the following command to stop all DNS lookups from the router CLI.

CustomerRouter(config)#**no ip domain-lookup**

Save the running configuration to the startup configuration.

CustomerRouter(config)#**end**
CustomerRouter#**copy run**
start

Step 6: Verify the configuration.

a. Log out of your terminal session with the Cisco 1841 customer router.
b. Log in to the Cisco 1841 Customer Router. Enter the console password when prompted.
c. Navigate to privileged EXEC mode. Enter the privileged EXEC password when prompted.
d. Click the **Check Results** button at the bottom of this instruction window to check your work.

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result:

Thus a network is established and the basic configurations are performed.

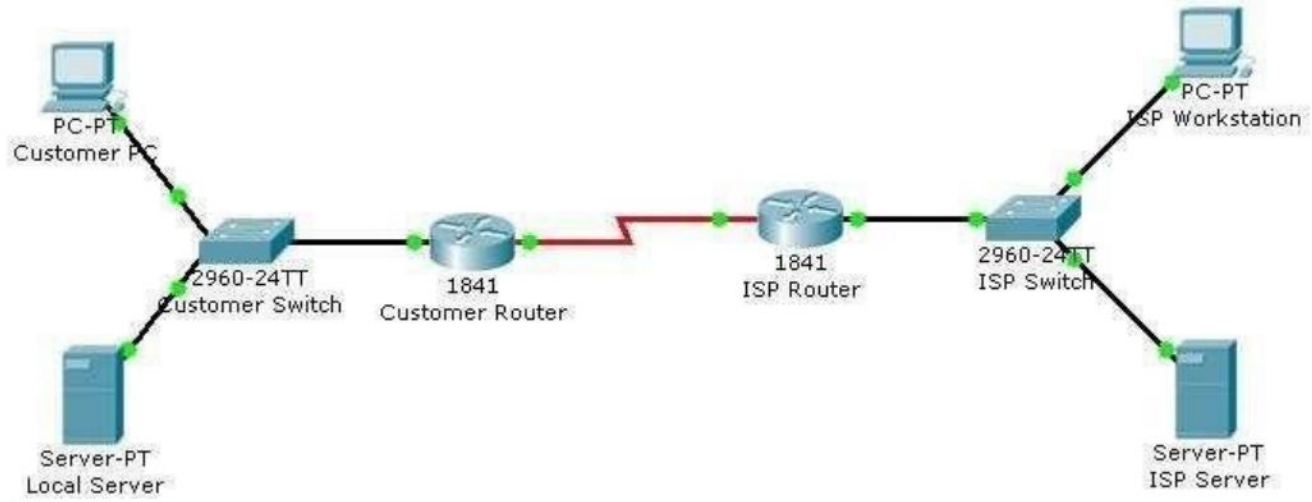
Ex.No. : 7 **Router Serial Interface Configuration**

Date :

Aim:

To configure Router Serial Interface using Cisco Packet Tracer.

Topology Diagram :



Objectives

- Perform an initial configuration of a Cisco Catalyst 2960 switch.

Background / Preparation

In this activity, you will configure these settings on the customer Cisco Catalyst 2960 switch:

- Host name
- Console password
- vty password
- Privileged EXEC mode password
- Privileged EXEC mode secret
- IP address on VLAN1 interface
- Default gateway

Step 1: Configure the switch host name.

a. From the Customer PC, use a console cable and terminal emulation software to connect to theconsoleof the customer Cisco Catalyst 2960 switch.

b. Set the host name on the switch to **CustomerSwitch** using these commands.Switch>**enable**

Switch#**configure terminal**

Switch(config)#**hostname CustomerSwitch**

Step 2: Configure the privileged mode password and secret.

a. From global configuration mode, configure the password as **cisco**.

CustomerSwitch(config)#**enable password cisco**

b. From global configuration mode, configure the secret as **cisco123**.

CustomerSwitch(config)#**enable secret cisco123**

Step 3: Configure the console password.

a. From global configuration mode, switch to configuration mode to configure the console line.

CustomerSwitch(config)#**line console 0**

b. From line configuration mode, set the password to **cisco** and require the password to beentered atlogin.

CustomerSwitch(config-line)#**password cisco**
CustomerSwitch(config-line)#**login**
CustomerSwitch(config-line)#**exit**

Step 4: Configure the vty password.

a. From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

CustomerSwitch(config)#**line vty 0 15**

b. From line configuration mode, set the password to **cisco** and require the password to beentered atlogin.

CustomerSwitch(config-line)#**password cisco**
CustomerSwitch(config-line)#**login**
CustomerSwitch(config-line)#**exit**

Step 5: Configure an IP address on interface VLAN1.

From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address192.168.1.5 with the subnet mask of 255.255.255.0.

CustomerSwitch(config)#**interface vlan 1**

CustomerSwitch(config-if)#**ip address 192.168.1.5 255.255.255.0**

CustomerSwitch(config-if)#**no shutdown**

CustomerSwitch(config-if)#**exit**

Step 6: Verify the configuration.

The Customer Switch should now be able to ping the ISP Server at 209.165.201.10. Thefirst one or two pingsmay fail while ARP converges.

CustomerSwitch(config)#**end**

CustomerSwitch#**ping 209.165.201.10**

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

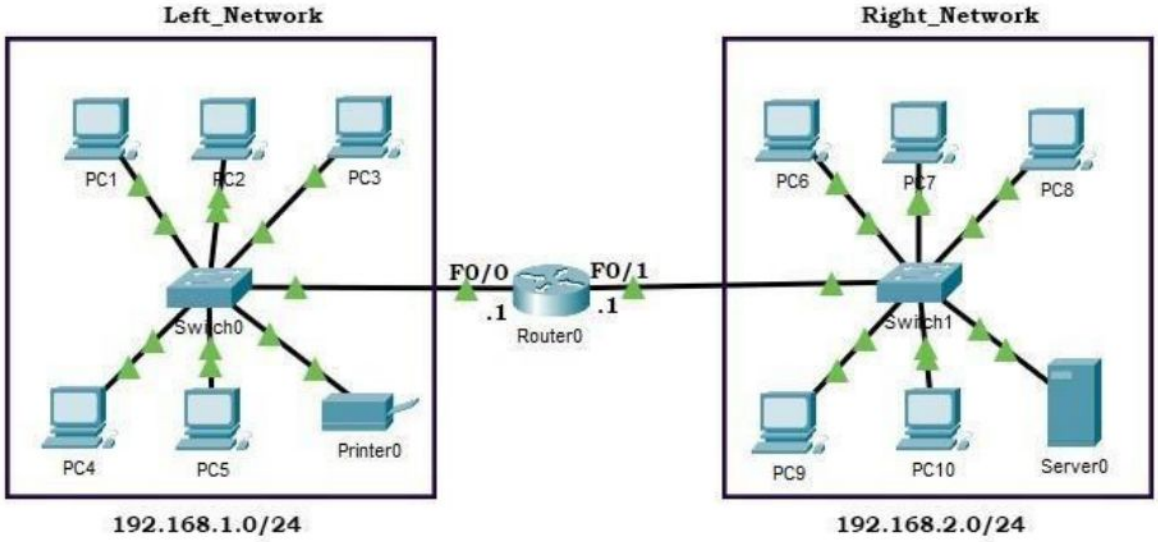
Activate the serial and ethernet addresses an assign appropriate addresses to the device interfaces is configured successfully.

Ex.No. : 8 **Configure the DHCP configurations in the respective**

routersDate :

Aim :

To configure DHCP configuration in the respective routers



Configuration	**Left_Network**	**Right_Network**
IP addresses	192.168.1.0 to 192.168.1.255	192.168.2.0 to 192.168.2.255
Available IP addresses for hosts	192168.1.10 to 192.168.1.254	192.168.2.10 to 192.168.2.254
Subnet mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	192.168.2.1
DNS Server	192.168.1.2	192.168.2.2
TFTP Server	192.168.1.3	192.168.2.3
Reserved	192.168.1.4 to 192.168.1.10	192.168.2.4 to 192.168.2.10

Configuring IP configuration on the router

A router connects different networks. If a router is connected to a network, hosts of the networkuse the router as the default gateway to reach the host of other networks.

In our example, since the **Left_Network** and **Right_Network** are respectively connected to the**Fast Ethernet 0/0** and **0/1** interfaces of the router, both networks will use the IP addresses of their respective interfaces as the default gateway IPs.

In simple terms, **Fast Ethernet 0/0** and **Fast Ethernet 0/1** of the router are the default gateways of the **Left_Network** and **Right_Network** respectively. Before configuring the router to act as a DHCP server, we have to configure and enable these interfaces.

To configure and enable these interfaces, access the command prompt of the router, and execute the following commands.

Router>enable
Router# configure terminal
Router(config)# interface FastEthernet
0/0
Router(config-if)# ip address 192.168.1.1
255.255.255.0Router(config-if)# no shutdown
Router(config-if)#exit
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip address 192.168.2.1
255.255.255.0Router(config-if)# no shutdown
Router(config-if)#exit

The following image shows the above commands on the packet tracer.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configuring DHCP server on the router

For each network that will obtain IP configuration from the DHCP server, we have to create andconfigure a DHCP pool on the router. In our example, we have two networks, so we have to create two DHCP pools, one for each network.

Use the following commands to create and configure a DHCP pool for the

Left_Network.Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.1.0 192.168.1.10
Router(config)#ip dhcp pool Left_Network
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.2
Router(dhcp-config)#option 150 ip 192.168.1.3

```
Router(dhcp-config)#network 192.168.1.0
255.255.255.0Router(dhcp-config)#exit
```

The following table describes the above commands.

Command	**Description**
ip dhcp excluded-address *192.168.1.0* *192.168.1.10*	This command tells the DHCP server not to assign the addresses from **192.168.1.0** to **192.168.1.10** to DHCP clients.
ip dhcp pool *Left_Network*	This command creates a DHCP pool named, **Left_Network** and changes command mode to DHCP pool configuration mode.
default-router *192.168.1.1*	This command assigns the default gateway to clients of this DHCP pool.
dns-server *192.168.1.2*	This command sets a primary DNS server for the clients.
option *150* ip *192.168.1.3*	This command provides the IP address of the TFTP server to the clients.
network *192.168.1.0* *255.255.255.0*	This command specifies the range of IP addresses for the pool.
exit	This command exits DHCP pool configuration mode.

Create and configure a DHCP pool for the Right_Network using the same commands as shownbelow.

```
Router(config)#ip dhcp excluded-address 192.168.2.0 192.168.2.10
Router(config)#ip dhcp pool Right_Network
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.2
Router(dhcp-config)#option 150 ip 192.168.2.3
Router(dhcp-config)#network 192.168.2.0
255.255.255.0Router(dhcp-config)#exit
Router(config)#
```

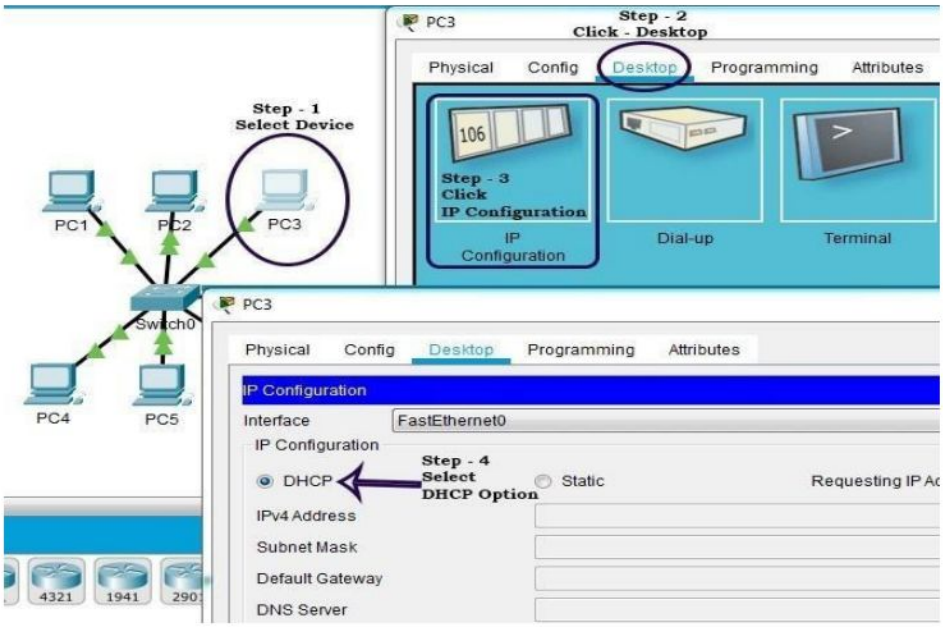
The following image shows how to execute the above commands on the router.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.1.0 192.168.1.10
Router(config)#ip dhcp pool Left_Network
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.2
Router(dhcp-config)#option 150 ip 192.168.1.3
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.2.0 192.168.2.10
Router(config)#ip dhcp pool Right_Network
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.2
Router(dhcp-config)#option 150 ip 192.168.2.3
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#exit
Router(config)#
```

Configuring DHCP clients

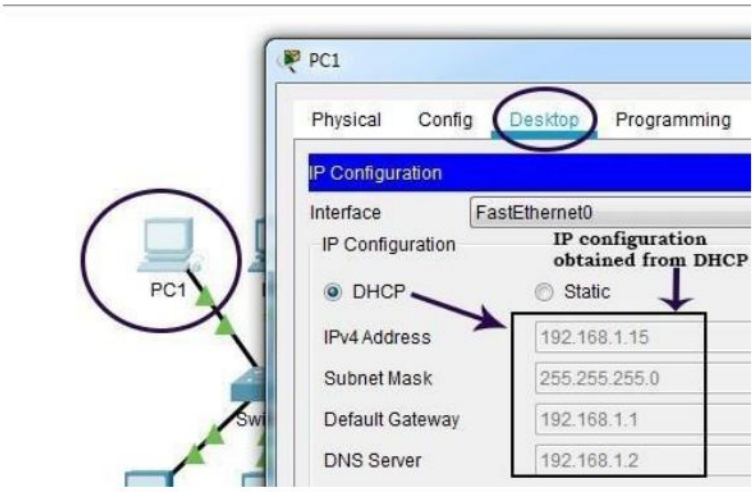
To configure a device as a DHCP client, change its IP configuration option to DHCP. To do this,click the device. In opened Windows, click the IP configuration option from the Desktop menu and set the IP configuration option to DHCP.

The following image shows the above procedure.

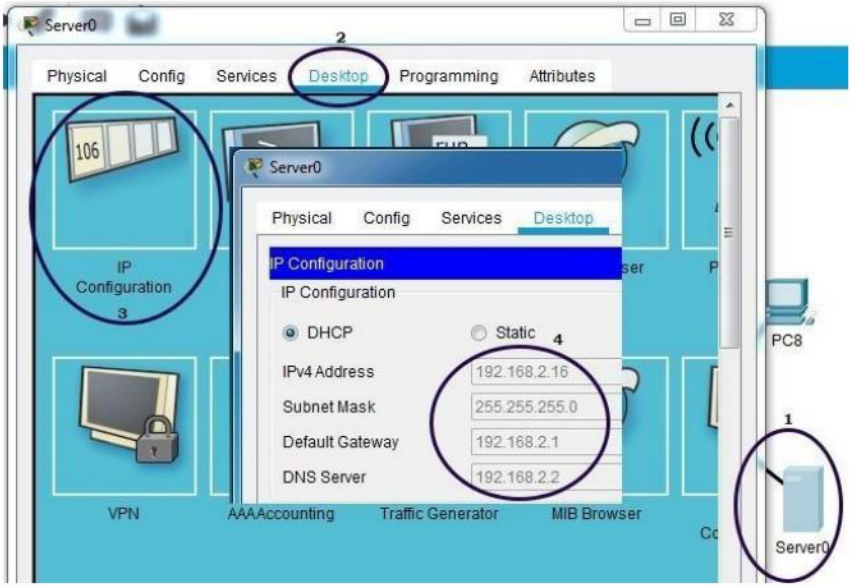


Verifying DHCP clients

To verify that the client has obtained IP configuration from the DHCP server, you can check theIP configuration option of the client again. For example, the following image shows how to verify this on a host of the Left_Network.



The following image shows how to verify this on a host of the **Right_Network**.



Verifying the DHCP Server

To verify that the DHCP server is working properly and to see the IP addresses that are provided by the DHCP server, run the following command in privileged-exec mode.

#ip dhcp binding

The following image shows the output of this command.

```
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.11     0002.4A7B.44EA          --                      Automatic
192.168.1.12     00D0.BC7C.BAB3          --                      Automatic
192.168.1.13     00E0.F76A.90C1          --                      Automatic
192.168.1.14     00D0.5884.22DC          --                      Automatic
192.168.1.15     00D0.BC31.67C3          --                      Automatic
192.168.1.16     0090.2B27.E90B          --                      Automatic
192.168.2.11     000C.8564.9677          --                      Automatic
192.168.2.12     0010.1171.4322          --                      Automatic
192.168.2.13     0004.9A93.BAA7          --                      Automatic
192.168.2.15     0030.F282.C8E7          --                      Automatic
192.168.2.14     0001.63D3.74B4          --                      Automatic
192.168.2.16     0000.0C8A.1542          --                      Automatic
Router#
```

To view detailed information about a specific DHCP pool, use the following command.

#show ip dhcp pool [pool-name]

For example, the following commands list the detailed information about the DHCP pools:Left_Network and Right_Network, respectively.

#show ip dhcp pool Left_Network
#show ip dhcp pool Right_Network

The following image shows the output of the above commands.

```
Router#show ip dhcp pool Left_Network
Pool Left_Network :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     6    / 2     / 254
Router#show ip dhcp pool Right_Network
Pool Right_Network :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.2.1          192.168.2.1      - 192.168.2.254     6    / 2     / 254
Router#
```

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

The configuration of a DHCP router is performed successfully using packet tracer.

Ex.No. : 9 **CONFIGURE THE PORT SECURITY FOR THE PORTS**
Date : **CONNECTED TO THE SWITCHES**

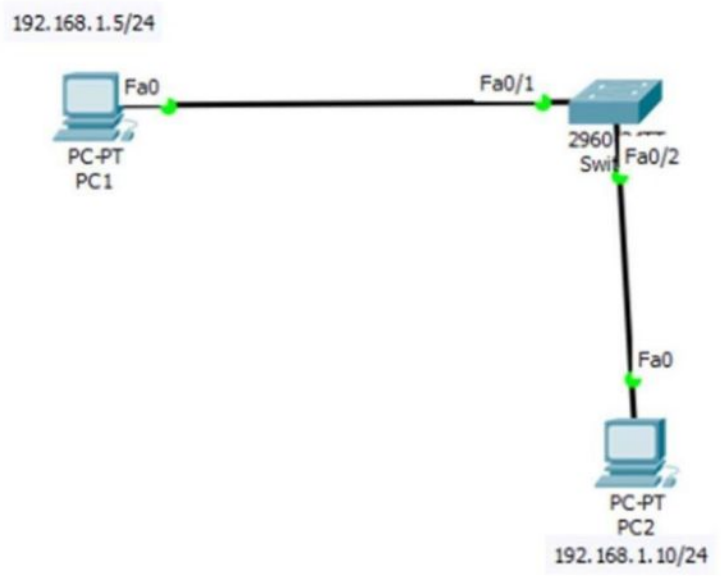
Aim :

To enable the port security for the ports connected to the switches.

Introduction :

Switch port Security is a **network security** feature that associates specific MAC addresses of devices(such as PCs) with specific interfaces on a switch. This will enable you to restrict accessto a given switch interface so that only the authorized devices can use it. If an unauthorizeddevice is connected to the same port, you can define the action that the switch will take, such as discarding the traffic, sending an alert, or shutting down the port.

1. Build the network topology:



PC1 connects to fa0/1 and PC2 to fa0/2 of the switch

2. Now configure switch port security on switch interfaces.

We'll configure port security interfaces on fa0/1 and fa0/2. To do this, we'll:

- Configure the port as an **access port**
- Enable **port security**
- Define which **MAC addresses** are allowed to send frames through this interface.

```
Switch(config)#int fa0/1
Switch(config-if)#switchport
mode accessSwitch(config-
if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
```

The *sticky* keyword instructs the switch to **dynamically** learn the MAC address of the currentlyconnected host.

Add these two optional commands.

- Defining the action that the switch will take when a frame from an unathorized device is received. This is done using the switchport port-security violation {protect | restrict | shutdown}interface command. All three options discard the traffic from the unauthorized device.
- Defining the maximum number of MAC addresses that can be received on the port using the switchport port-security maximum NUMBER interface submode command

Let's add the above 2 commands to our configuration:

```
Switch(config-if)#switchport port-security
violation shutdownSwitch(config-if)#switchport
port-security maximum 1
```

We're are done with port security configuration for fa0/1

In a similar way to switch interface *fa0/1*, configure switch port security for *fa0/2* connectedto PC2**:**

```
Switch(config)#interface fa0/2
Switch(config-if)#switchport
mode accessSwitch(config-
if)#switchport port-security
Switch(config-if)#switchport port-security mac-
address sticky Switch(config-if)#switchport port-
security violation shutdown Switch(config-
if)#switchport port-security maximum 1
```

That's all for port-security configuration on fa0/2

A shorthand method for configuration**:**The port security configurations for both fa0/1 and fa0/2could be done more faster with the help of interface range command as shown below:

```
Switch(config-if-range)#interface
range fa0/1-2Switch(config-

if)#switchport mode access
Switch(config-if)#switchport port-
security
Switch(config-if)#switchport port-security mac-
```

address sticky Switch(config-if)#switchport port-security violation shutdown Switch(config-if)#switchport port-security maximum 1

Here, we define a range of interfaces on which we want to configure port security, then proceedto configure port-security for all the interfaces specified at a go instead of one interface at a time.

The interface range command can save you tons of work in doing individual configurations ifyou were configuring port security for many switch interfaces, say, 24 ports on a switch.

Next,

4. We'll verify port security configurations on interfaces fa0/1 and fa0/2

To verify if the switch has learnt the MAC address of PC1, you can use the command:

show port-security interface fa0/1

```
Switch#
Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0005.5E57.A982:1
Security Violation Count   : 0
```

Verify that the switch has learnt the MAC address of PC1.

You may also use the command: show port-security

address

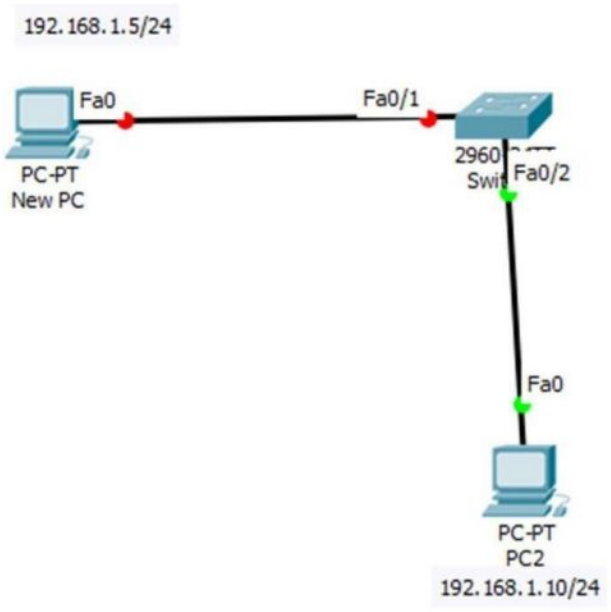
```
Switch#show port-security address
                                          Secure Mac Address Table
------------------------------------------------------------------------
--------------
Vlan       Mac Address Type                                       Ports
           Remaining Age

                     (mins)
----       ----------- ----                                       -----
           -------------
1          0005.5E57.A982         SecureSticky
FastEthernet0/1                   -
1          0007.EC08.B84C         SecureSticky
FastEthernet0/2                   -
------------------------------------------------------------------------
-------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Try also pinging PC2 from PC1. Ping should be successful here since switch port security is notviolated.

The case of Port Security Violation

Now connect a different PC to fa0/1 in place of PC1. See the effect of doing this:



Notice that fa0/1 shuts down upon connecting the new PC, as indicated by the red LED.

This is because the switch had already associated fa0/1 with the MAC address of PC1 and the **maximum** number of MAC addresses that we defined for this port is **1**. So attaching the new PC to fa0/1 violates the port security rules that we set and as a result, the interface **shuts down**.

You can verify this further by using the command we used before: show port-security interfacefa0/1

```
Switch#
Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.64C3.8971:1
Security Violation Count   : 1
```

Verify from above that **port status** is now **Secure-shutdown** upon violation of port security.

Further, a ping from the New PC to PC2 will definitely fail because the switch cannot forward aframe via an interface that is shut down.

How to Reset an interface that has been shut down due to Violation of Port Security:

One of the options on the table is to manually restart the shutdown interface(fa0/1 in our case here). Unplug the cable from unauthorized PC(new PC) and plug it back to authorized PC(PC1)

Then run following commands on switch and test connectivity from the authorized PC (PC1):

Switch(config)#interface
fa0/1 Switch(config-
if)#shutdown
Switch(config-if)#no
shutdown

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result:

Thus the port security for the ports connecte d to switched is successfully performed.

Ex.No.: 10 **Configure the access list in Routers**

Date :

Aim:

To configure the access list in Routers

IP ACL types

Two types of IP ACL can be configured in Cisco Packet Tracer 7.2 :

- **Standard ACLs** : This is the oldest ACL type which can be configured on Cisco routers.Traffic is filtered based on the source IP address of IP packets. The access-list number can be any number from 1 to 99. This kind of ACL has to be placed near the destination to avoid blocking legitimate trafic from the source.

access-list 1 permit 10.2.25.0
0.0.0.255access-list 1 deny any

- **Extended ACLs :** Introduced in IOS version 8.3, the extended ACLs are more complex and allow filtering of the IP traffic based on a combination of multiple criterias : source IP address, destination IP address, TCP or UDP port, protocol, In numbered ACLs, the
access-list number can be any number from 100 to 199 or 2000 to 2699 (available in IOSversions >12.0.1). Such ACLs can also be named access lists in which the ACL number is replaced by a keyword. This kind of ACL has to be placed near the source as it allows fine grained control to ressources accessed. Placing the ACL near the destination will make the trafic travel through the network before beeing blocked, resulting in bandwidth waste.

access-list 1 permit ip 10.2.25.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 101 permit icmp any 10.1.0.0 0.0.255.255
echoaccess-list 1 deny ip any any

Configuration on Cisco 2911 ISR Router

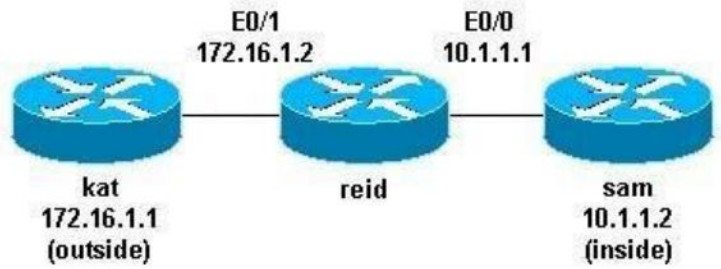
Restrict remote telnet or SSH access to the ISR router

access-list 1 permit 192.168.1.0 0.0.0.255

line vty 0 4
access-class 1 in
login

```
line vty 5 15
 access-class 1 in
 login
```

Network Diagram



Standard ACLs

Standard ACLs are the oldest type of ACL. They date back to as early as Cisco IOS Software Release 8.3. Standard ACLs control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL.

This is the command syntax format of a standard ACL.

access-list *access-list-number* **{permit|deny}**
{*host|source source-*
*wildcard***|any}interface**
<*interface***>**
ip access-group number {in|out}

This is an example of the use of a standard ACL in order to block all traffic except that from source 10.1.1.x.

```
interface Ethernet0/0
ip address 10.1.1.1
255.255.255.0ip access-
group 1 in
access-list 1 permit 10.1.1.0 0.0.0.255
```

Extended ACLs

This is the command syntax format of extended ACLs. Lines are wrapped here for spacing considerations.

IP

access-list *access-list-number*
[dynamic *dynamic-name* **[timeout** *minutes***]]**
{deny|permit} *protocol source source-wildcard destination destination-wildcard*

[precedence *precedence*][**tos** *tos*] **[log|log-input] [time-range** *time-range-name*]

ICMP

access-list *access-list-number*
[dynamic *dynamic-name* **[timeout** *minutes*]]
{deny|permit} icmp *source source-wildcard destination destination-wildcard*
[*icmp-type* [*icmp-code*] |*icmp-message*]
[precedence *precedence*] **[tos** *tos*]
[log|log-input][time-range *time-range-name*]

interface <*interface*>
ip access-group {*number|name*}
{in|out}interface Ethernet0/1
ip address 172.16.1.2 255.255.255.0
ip access-group 101 in
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 101 permit ip any 10.1.1.0 0.0.0.255

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

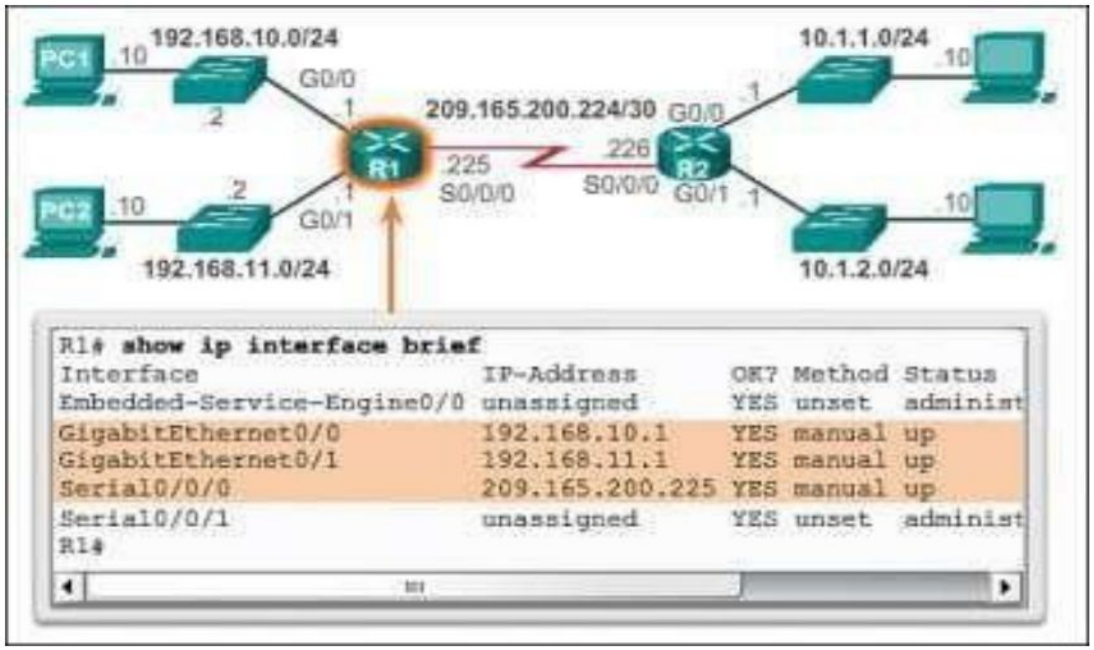
Thus the access list in routers is configured s ccessfully.

Ex.No. : 11 **Verify Connectivity of Directly Connected Networks**

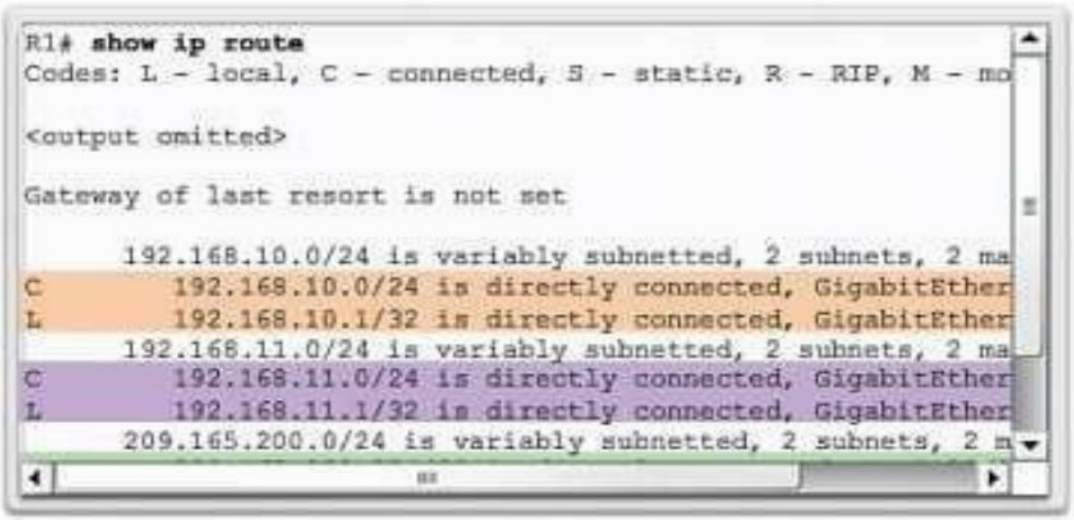
Date :

Aim :

To verify connectivity of directly connected networks



Tthe output of the **show ip route** command.



```
R1# show running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 128 bytes
!
interface GigabitEthernet0/0
 description Link to LAN 1
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
end

R1#
```

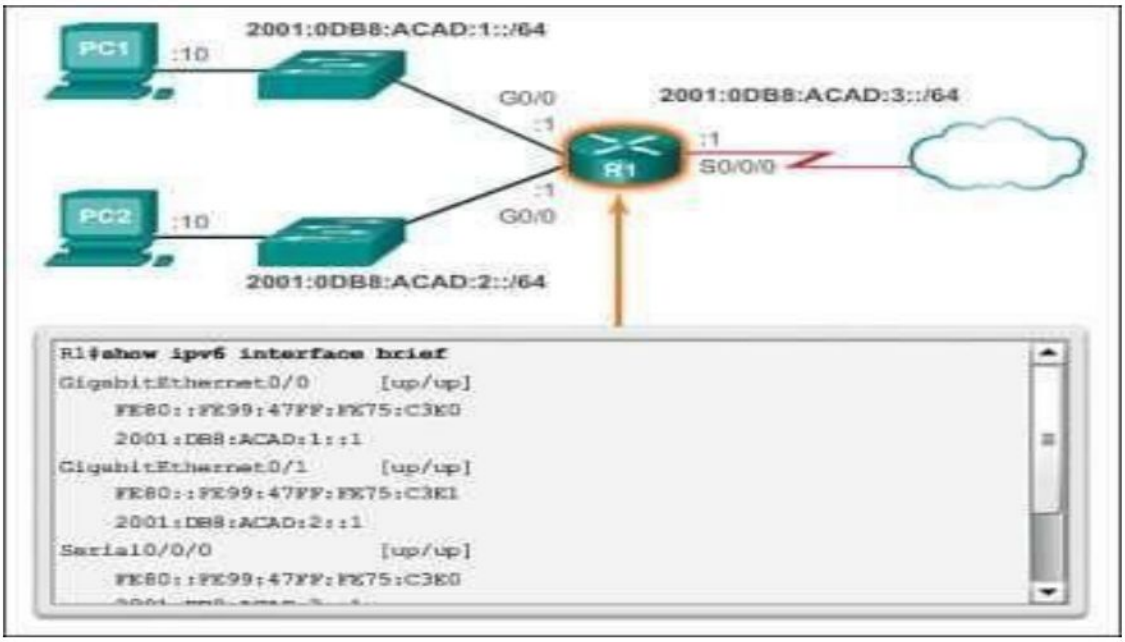
Verify an Interface Configuration

The following two commands are used to gather more detailed interface information:

- **show interfaces**: Displays interface information and packet flow count for all interfaceson the device
- **show ip interface**: Displays the IPv4-related information for all interfaces on a router

Go to the online course to use the Syntax Checker in the fourth and fifth graphics to verify theinterfaces of the R2 router.

Verify IPv6 Interface Settings



Verify the R1 IPv6 Interface Status

```
<output omitted>

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
```

Verify the R1 IPv6 Routing Table

```
R1#ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5)
R1#
```

Verify Connectivity on R1

Other useful IPv6 verification commands include:

- **show interface**
- **show ipv6 routers**

```
R1# show running-config | section line vty
line vty 0 4
 password 7 030752180500
 login
 transport input all
R1#
```

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ
R1#
R1# show ip interface brief | include up
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
R1#
```

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ

R1# show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up

R1#
```

Filter **show** Commands to Exclude Rows of Output

```
R1# show ip route | begin Gateway
Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

Result:

Thus the connectivity of all the devices of a LAN is verified successfully

Ex.No : 12 **Configure RIP Routing on the Router and verify theDate :**

configurations and connectivity

Aim :

To configure RIP routing on the router and verify the configurations and connectivity

Configuring RIP in Packet Tracer

1. Build the network topology.

2. Configure IP addresses on the PCs and the routers.

Router 1

R1(config)#
R1(config)#int
fa0/0
R1(config-if)#ip address 10.0.0.1
255.0.0.0R1(config-if)#no shut

R1(config-if)#
R1(config-if)#int serial 0/0/0
R1(config-if)#ip add 20.0.0.1
255.0.0.0R1(config-if)#no shut

Router 2

R2(config)#
R2(config)#int
fa0/0
R2(config-if)#ip add 30.0.0.1
255.0.0.0R2(config-if)#no shut

R2(config-if)#
R2(config-if)#int serial 0/0/0
R2(config-if)#ip add 20.0.0.2
255.0.0.0R2(config-if)#no shut

IP configuration on PCs

Click PC->Desktop->IP Configuration. On each PC assign these addresses: **PC1**: IP address: 10.0.0.2 Subnet mask 255.0.0.0 Default Gateway 10.0.0.1 **PC2**: IP address: 30.0.0.2 Subnet mask 255.0.0.0 Default Gateway 30.0.0.1 And now:

3. Configure **RIPv2** on the routers

Router 1

R1(config)#

R1(config)#router rip
R1(config-
router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 20.0.0.0

Router 2

R2(config)#

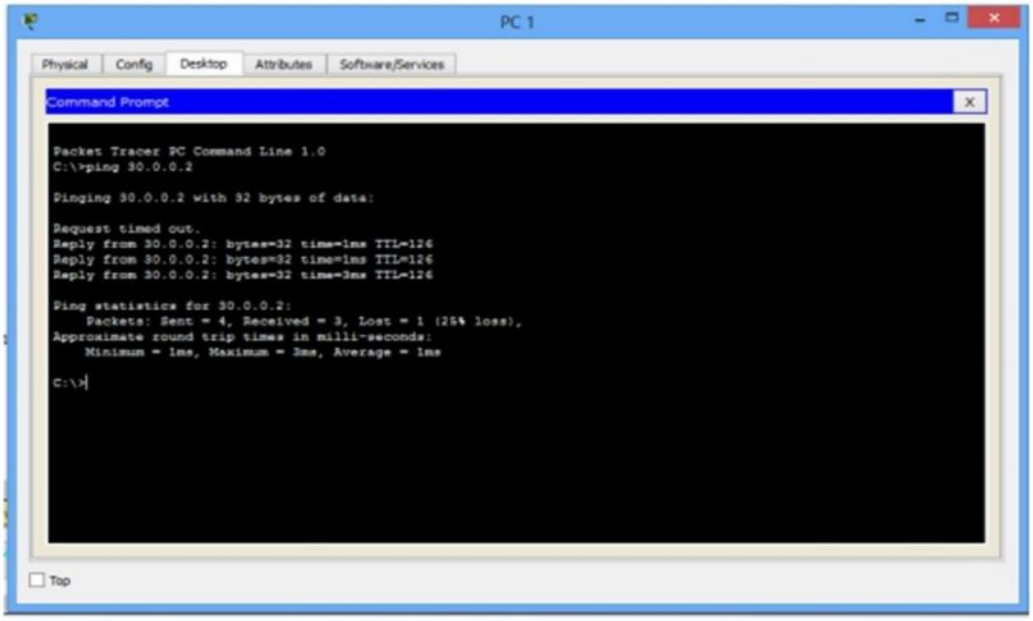
R2(config)#router rip
R2(config-

router)#version 2
R2(config-router)#network 20.0.0.0
R2(config-router)#network 30.0.0.0

4. Now **verify** RIP configuration.

To verify that RIP is in deed advertising routes,we can use the *show ip route* command on **R1.**

- Ping **PC2** from **PC1** to further confirm that connectivity is really established betweenthe two subnets.



Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

Thus the configuration of RIP routing the router is successfully completed.

Content Beyond the syllabus

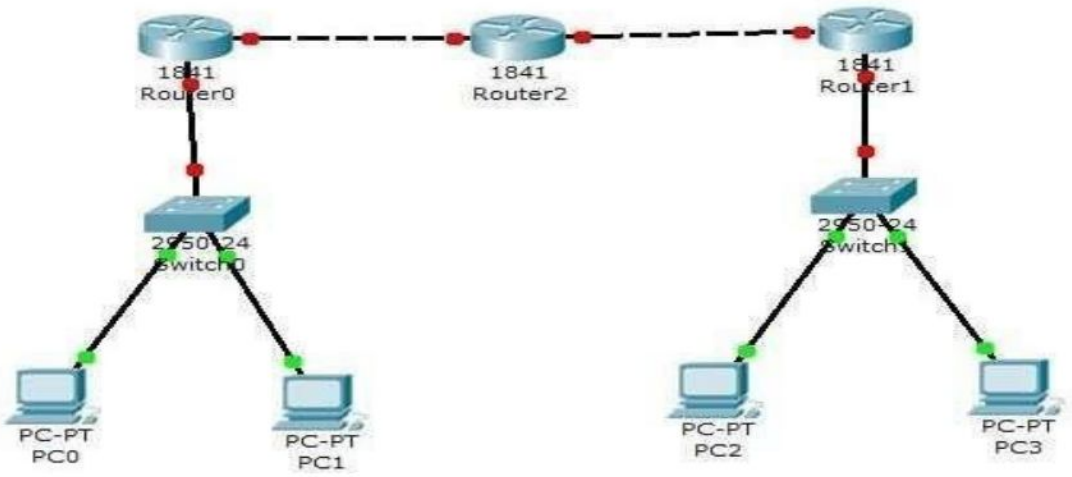
Ex. No. 13 **Configure a Network topology**

Date :

Aim: Configure a Network topology using packet tracer software.

Procedure: To implement this practical following network topology is required to beconfigured using the commands learned in previous practical.

After configuring the given network a packet should be ping from any onemachine to another.



Router0 Configuration Command :.....

Continue with configuration dialog? [yes/no]: no
Press RETURN to get
started! Router>
Router>Enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname router0
router0(config)#interface fastethernet
0/0router0(config-if)#ip address
192.168.1.1
255.255.255.0 router0(config-if)#description
router0 fastethernet 0/0 router0(config-if)#no
shutdown

```
%LINK-5-CHANGED: Interface FastEthernet0/0,
changedstate to up  router0(config-if)#exit
router0(config)#interface fastethernet 0/1
router0(config-if)#description router0
fastethernet0/1 router0(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1,
changedstate to up router0(config-if)#exit

router0(config)#exit

%SYS-5-CONFIG_I: Configured from console byconsole
router0#show running-config
Building configuration...

Current configuration : 437 bytes
interface FastEthernet0/0
description router0 fastethernet
0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto

interface FastEthernet0/1
description router0
fastethernet0/1 no ip address
duplex auto speed auto

interface Vlan1 no ip
 addressshutdown

line con 0
line vty 0 4
 login

router0
#
router0
#
router0#copy running-config startup-
config Destination filename
[startup-config]?
Building
configuration...
[OK]router0#
```

Dept. of IT

DESCRIPTION	Max Marks	Marks Obtained
AIM	10	
Software/Tools Required & Algorithm	10	
Coding/Programming & Execution	15	
Record	25	
Viva-voce	5	
Result	10	
Total	75	

Result :

Thus the network topology is configured using packet tracer.