ARAVALI COLLEGE OF ENGINEERING & MANAGEMENT

Jasana Tigoan Road Greater Faridabad Haryana, 121006

WORKSHOP-II
(Networking-File)
BCA-23-112

ARAVALI
COLLEGE OF ENGINEERING & MANAGEMENT
creating achievers

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
(2024-2025)

FACULTY INCHARGE:	SUBMITTED BY:
Ms. Mahima	**Ankit Kumar**
(Assistant Professor)	**Roll No:24011312010**

INDEX

Experiment-1

Aim: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.

Apparatus (Components): RJ-45 connector, Climping Tool, Twisted pair Cable

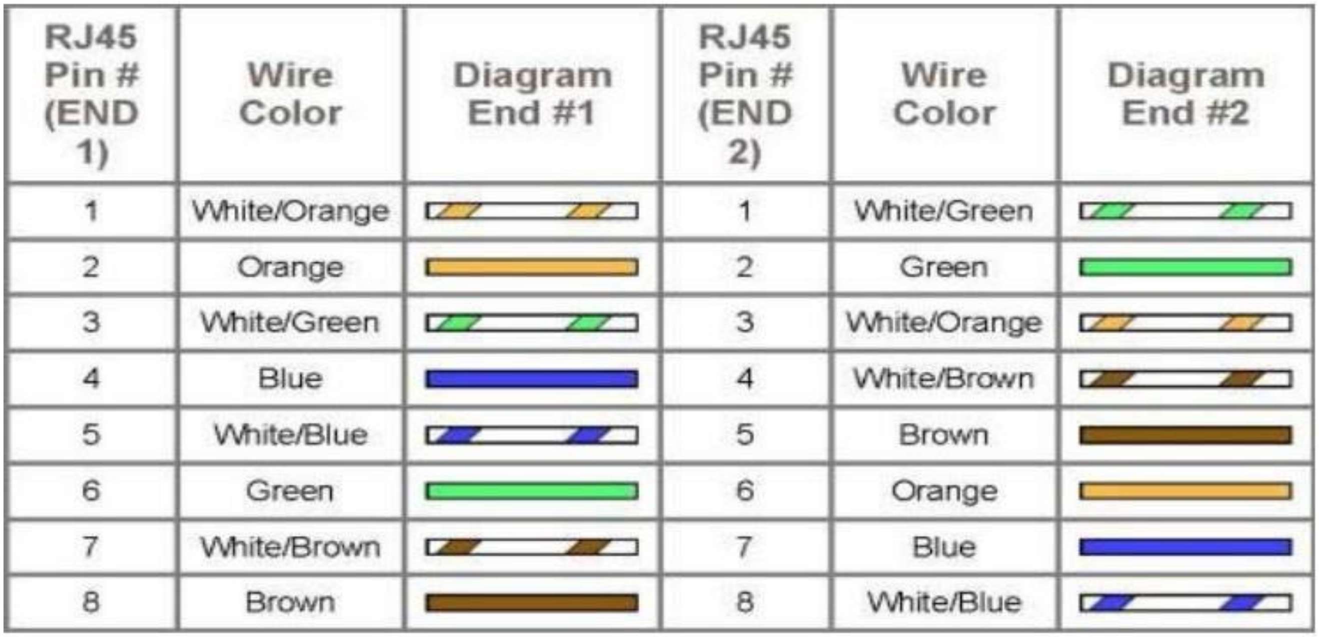
Procedure: To do these practical following steps should be done:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

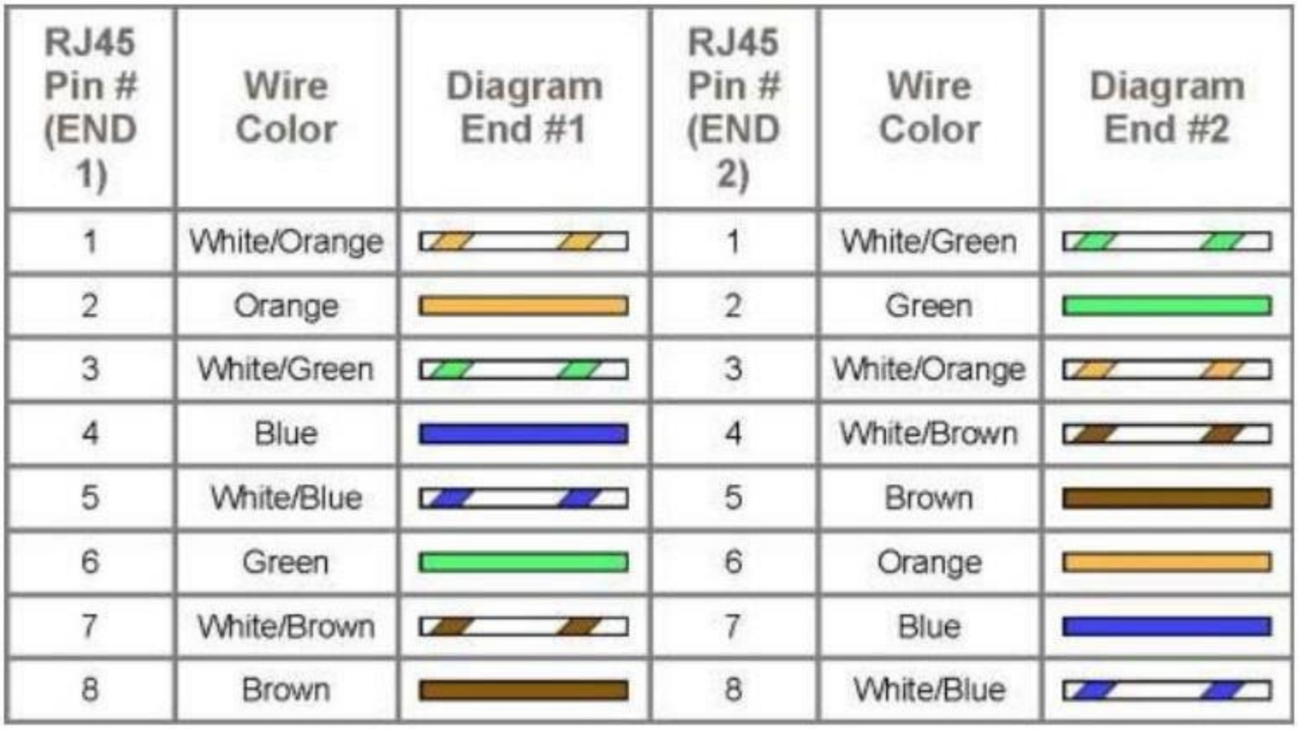
3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

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	▨

Experiment-2

Aim: Study of following Network Devices in Detail

- Repeater
- Hub
- Bridge
- Router
- Gate Way

Apparatus (Software): No software or hardware needed.

Procedure: Following should be done to understand this practical.

1. **Repeater:** Functioning at Physical Layer. A **repeater** is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports ,so cannot be use to connect for more than two devices

2. **Hub:** An Ethernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

3. **Bridge:** A **network bridge** connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term *bridge* formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports.

4. **Router:** A **router** is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another.

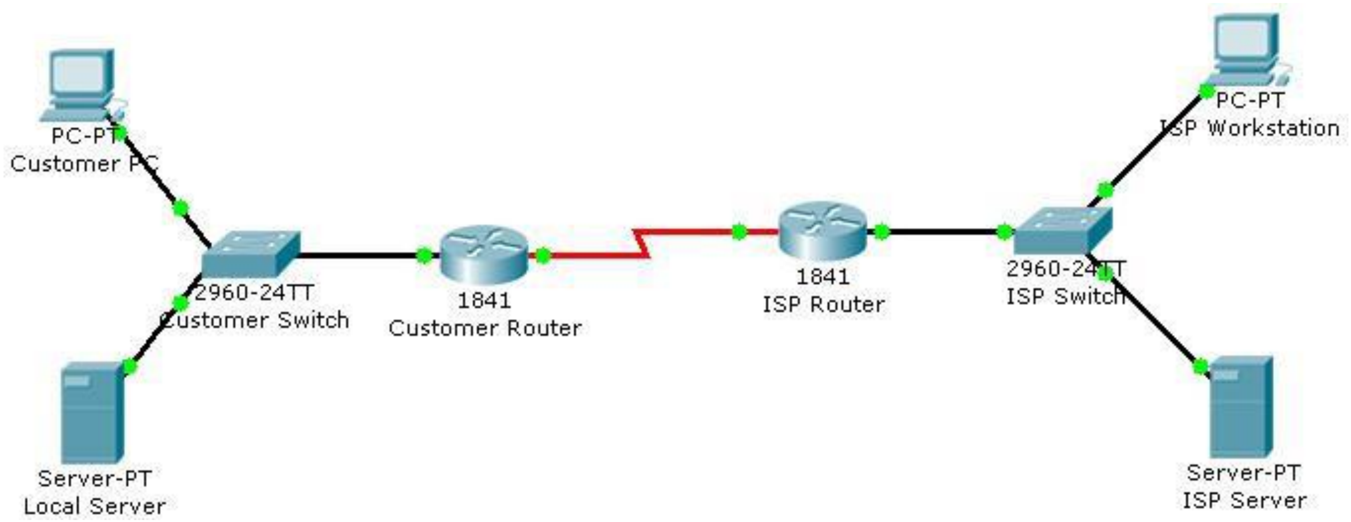
5. **Gate Way**: A **gateway** is a device or node that connects two different networks, allowing communication between them by translating protocols. It acts as an entry or exit point for data, ensuring seamless interaction between networks with different architectures.

Experiment-3

Aim: Performing an Initial Switch Configuration

Apparatus (Software): Command Prompt And 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

Note: Not all commands are graded by Packet Tracer.

Step 1: Configure the switch host name.

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

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

```
Switch>enable
Switch#configure t
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 be entered at login.

```
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 be entered at login.

Step 5: Configure an IP address on interface VLAN1.

From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address 192.168.1.5 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: Configure the default gateway.

a. From global configuration mode, assign the default gateway to 192.168.1.1.

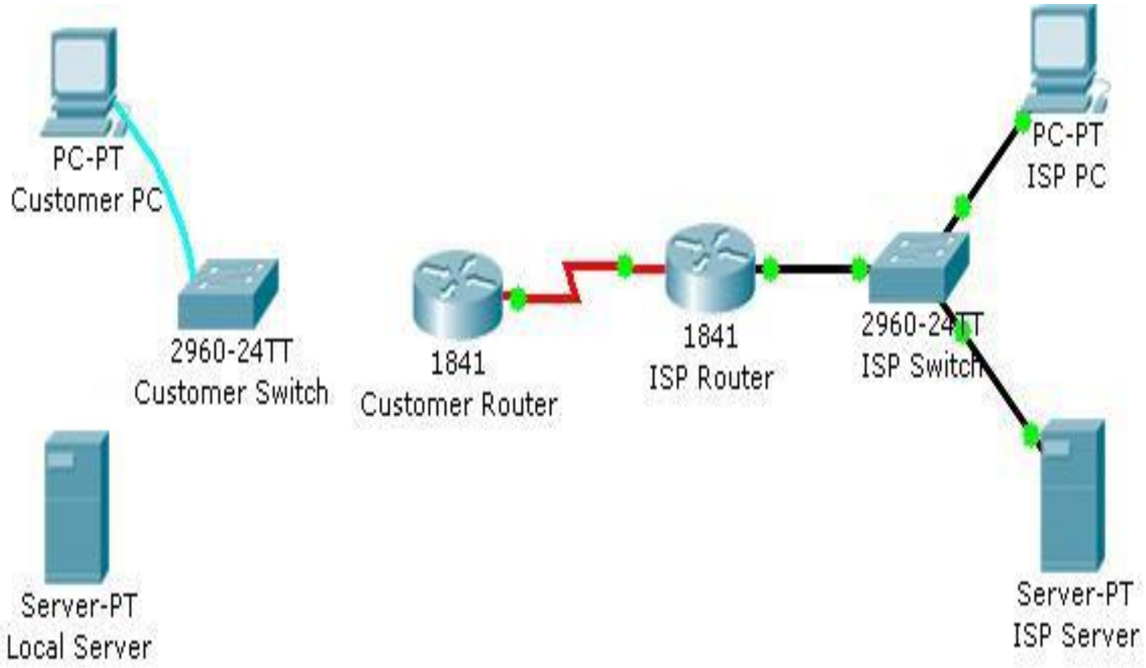
```
CustomerSwitch(config)#ip default-gateway 192.168.1.1
```

Experiment-4

Aim: Connecting and configuring Switch

Apparatus (Software): Command Prompt And Packet Tracer.

Topology Diagram



Objectives

- Connect a switch to the network.
- Verify the configuration on the switch.

Background / Preparation

In this activity, you will verify the configuration on the customer Cisco Catalyst 2960 switch. The switch is already configured with all the basic necessary information for connecting to the LAN at the customer site. The switch is currently not connected to the network. You will connect the switch to the customer workstation, the customer server, and customer router. You will verify that the switch has been connected and configured successfully by pinging the LAN interface of the customer router.

Step 1: Connect the switch to the LAN.

a. Using the proper cable, connect the FastEthernet0/0 on Customer Router to the FastEthernet0/1 on Customer Switch.

b. Using the proper cable, connect the Customer PC to the Customer Switch on port FastEthernet0/2.

c. Using the proper cable, connect the Local Server to the Customer Switch on port FastEthernet0/3.

Step 2: Verify the switch configuration.

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

b. Use the console connection and terminal utility on the Customer PC to verify the configurations. Use **cisco** as the console password.

c. Enter privileged EXEC mode and use the **show running-config** command to verify the following configurations. The password is **cisco123**.

    a. VLAN1 IP address = 192.168.1.5

    b. Subnet mask = 255.255.255.0

    c. Password required for console access

    d. Password required for vty access

    e. Password enabled for privileged EXEC mode

    f. Secret enabled for privileged EXEC mode

a. Verify IP connectivity between the Cisco Catalyst 2960 switch and the Cisco 1841 router by initiating a ping to 192.168.1.1 from the switch CLI.

b. Click the **Check Results** button at the bottom of this instruction window to check your work.

Experiment-5

Aim: To study, design, and implement various network topologies (bus, star, ring, and mesh) to understand their characteristics, advantages, and limitations.

Apparatus:

Cisco Packet Tracer software, PCs, switches, network cables, connectors.

Objectives:

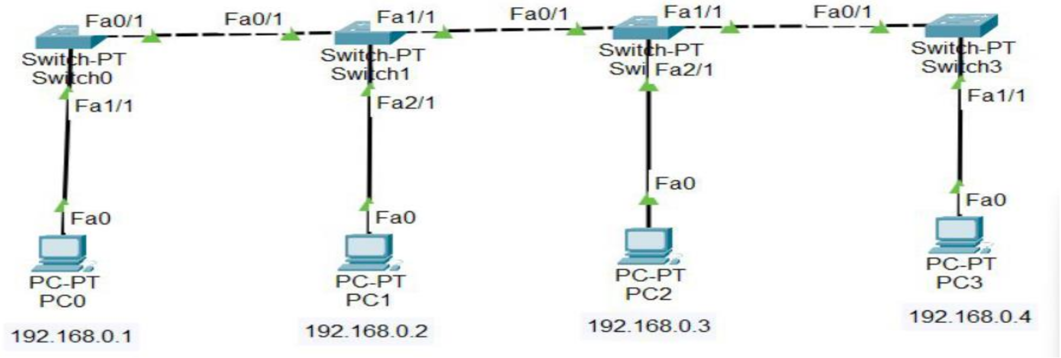
- Understand the characteristics and structure of bus, star, ring, and mesh topologies.
- Implement these topologies using simulation tools.
- Evaluate their reliability, scalability, and performance.

THEORY:

Network topology defines the physical or logical arrangement of nodes and connections in a network. It determines how data flows and impacts fault tolerance, scalability, and efficiency.

Procedure:

1. **Bus Topology Implementation:**

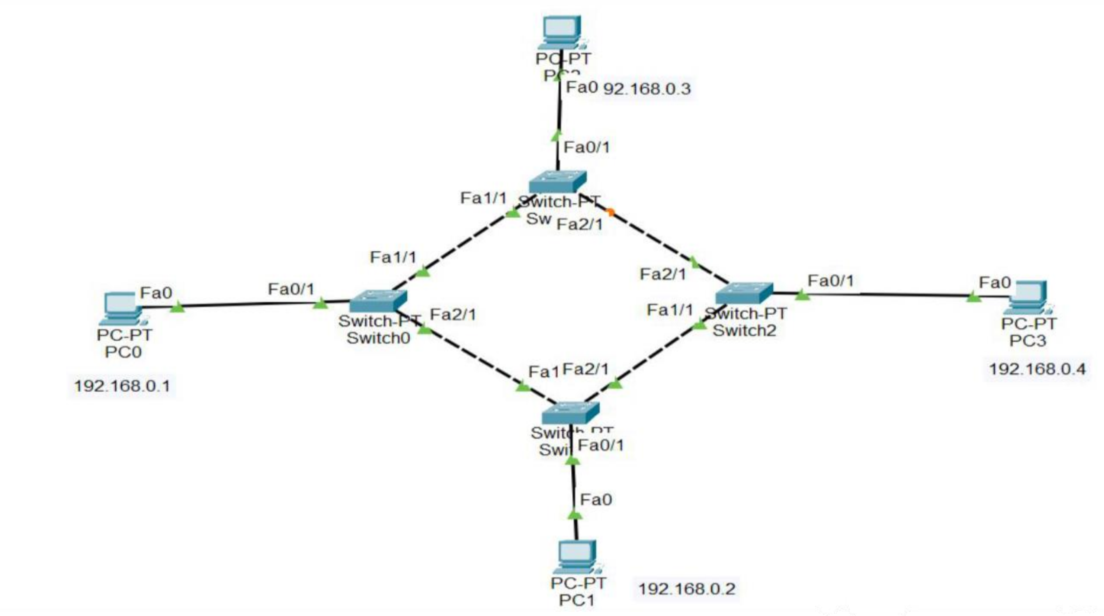


   - Place 5 PCs on the workspace and connect them using a single coaxial backbone cable.

   - Assign IP addresses within the range 192.168.1.x/24.
   - Test connectivity using the ping command.
   - Simulate a disconnection in the backbone cable and observe network failure.

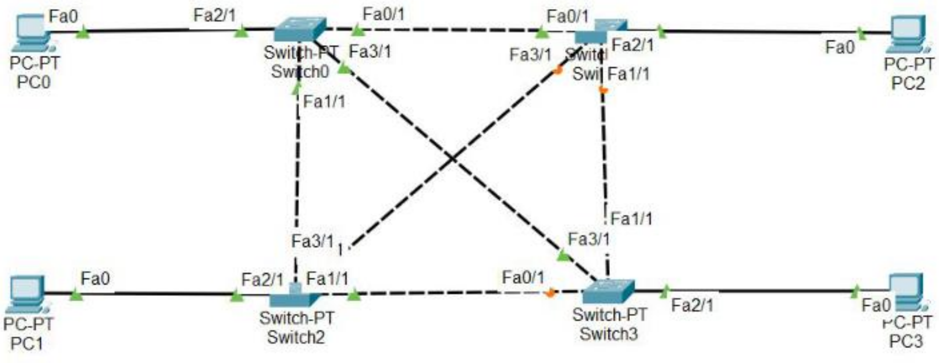
2. **Star Topology Implementation:**
   - Connect 5 devices to a central switch.
   - Assign IPs in the subnet 192.168.2.x/24.
   - Analyze the dependency on the central switch.

3. **Ring Topology Implementation:**



   - Connect each device to two others in a circular arrangement.
   - Assign IPs in the subnet 192.168.3.x/24.
   - Simulate a broken link and observe rerouting or disruption.

4. **Mesh Topology Implementation:**



   - Connect every device to all other devices directly.
   - Use IPs in the subnet 192.168.4.x/24.
   - Calculate the total connections using (n(n-1)/2).

Observations:

- Bus topology failed with a backbone cable disconnect.
- Star topology showed dependency on the central hub.
- Ring topology rerouted data effectively within certain limits.
- Mesh topology demonstrated high reliability but required significant resources.

Conclusion: Each topology is suited for specific use cases, with mesh offering the best reliability but at a higher cost.

Experiment-6

Aim: To design and implement different Local Area Network (LAN) configurations, including client-server, peer-to-peer, and hierarchical setups, to understand their applications.

Apparatus:

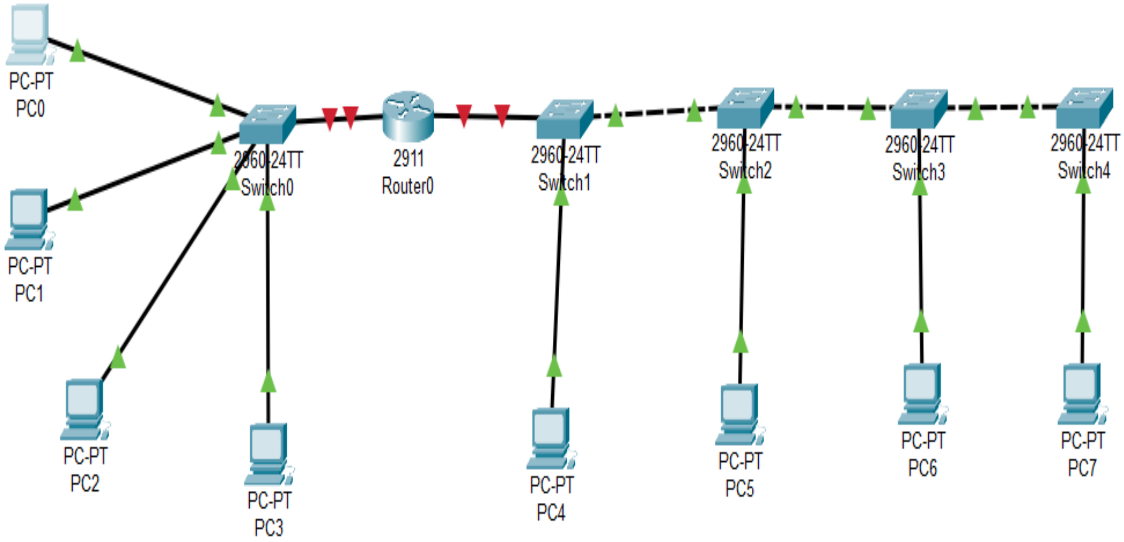
Cisco Packet Tracer, PCs, routers, switches, network cables.

Objectives:

- Develop LAN setups for specific networking needs.
- Implement VLANs to improve network segmentation.
- Analyze performance and resilience across different configurations.

THEORY:

LAN configurations depend on organizational requirements. While client-server networks centralize control, peer-to-peer networks focus on equal privileges. Hierarchical designs improve scalability through layered architecture



Procedure:

1. **Client-Server LAN Configuration:**
   - Set up a server with DHCP, DNS, and file-sharing roles.
   - Connect 5 PCs to a switch and link them to the server.
   - Assign IPs in the range 192.168.10.10
   - Test file and printer sharing between PCs.
2. **Peer-to-Peer LAN Implementation:**
   - Connect 4 computers to a switch using static IPs (192.168.20.x/24).
   - Enable file sharing on each computer.
   - Test connectivity and resource-sharing capabilities.
3. **Hierarchical LAN Design:**
   - Set up access, distribution, and core switches.
   - Create VLANs at the access layer.
   - Implement inter-VLAN routing at the distribution layer.
   - Connect devices to access switches and verify communication..

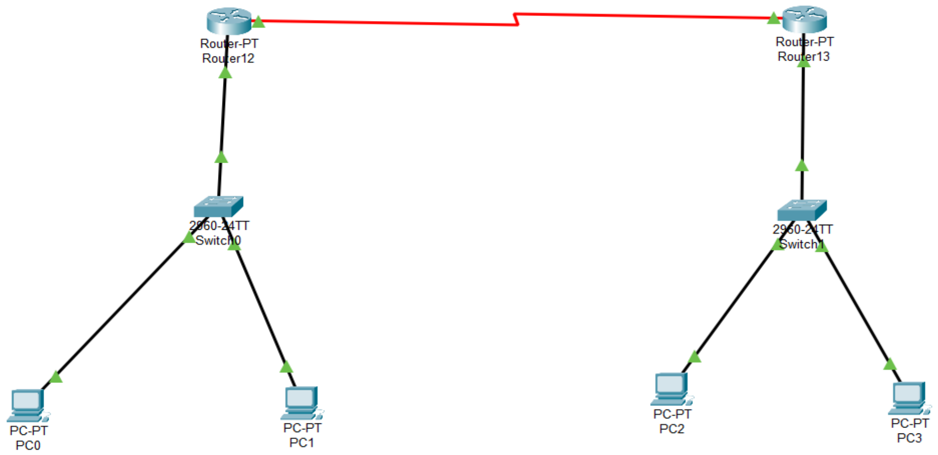
Conclusion:

Selecting an appropriate LAN configuration depends on the network's scale and resource requirements.

Experiment-7

Aim: To configure static routes on routers to enable communication between different networks.

Apparatus: Cisco Packet Tracer, two routers, PCs, and network cables.



Objectives:

- Configure IP addressing and static routes on routers.
- Establish communication between separate subnets.

THEORY:

Static routing involves manually defining paths for data to travel between networks. It is simple to implement but lacks adaptability to topology changes.

Procedure:

1. Configure Router1:
    - Set LAN IP: 192.168.1.1/24.
    - Set WAN IP: 10.0.0.1/30.

2. Configure Router2:
   - Set LAN IP: 192.168.2.1/24.
   - Set WAN IP: 10.0.0.2/30.
3. Add Static Routes:
   - Router1: Add route to 192.168.2.0/24 via 10.0.0.2.
   - Router2: Add route to 192.168.1.0/24 via 10.0.0.1.
4. Verify Routing:
   - Use ping to test communication between networks.

Observations:

Routing tables reflected the manually configured paths. Hosts from different networks successfully communicated.

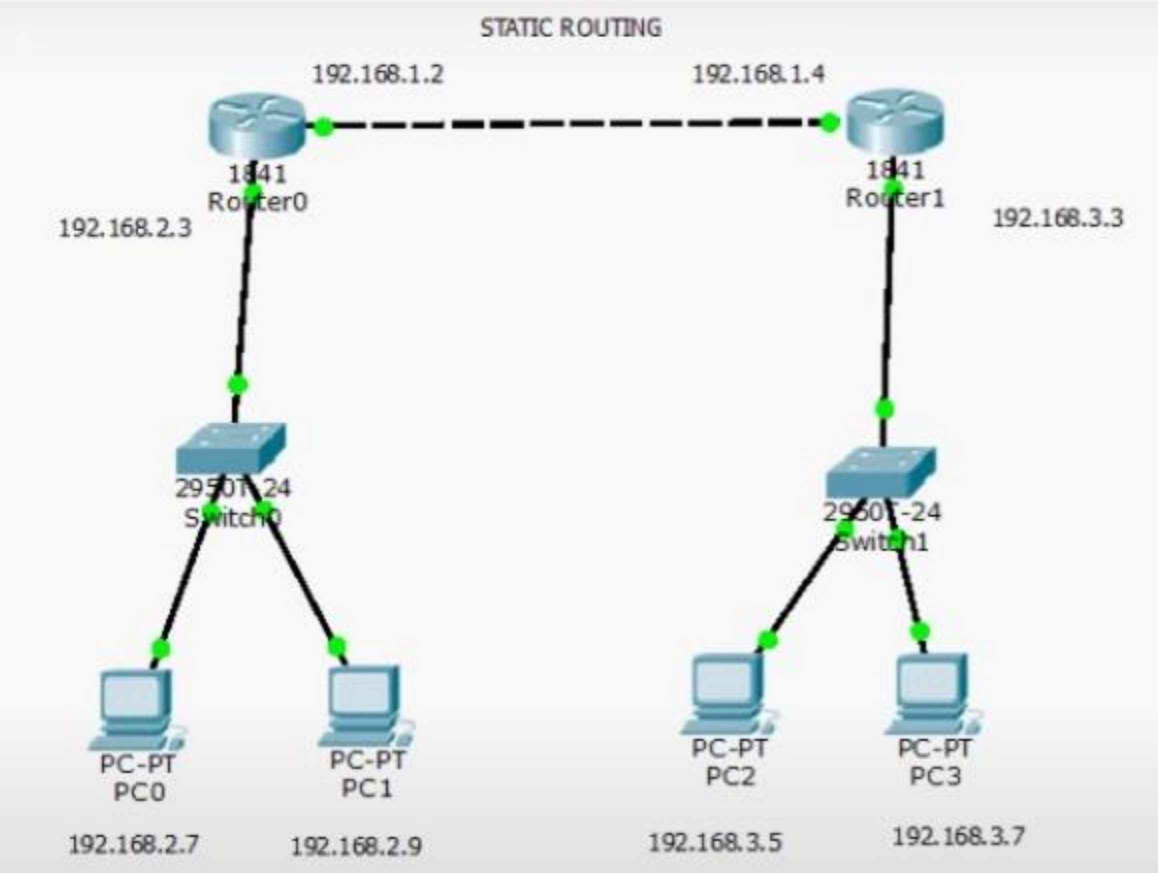
Conclusion:

Static routing ensures connectivity but requires updates for topology changes.

Experiment-8

Aim: To configure and compare network connectivity using static routing and dynamic routing protocols, analyzing their efficiency and adaptability.

Apparatus: Cisco Packet Tracer, three routers, PCs, network cables.



Objectives:

- Establish communication using static routing.
- Implement dynamic routing protocols like RIP.
- Compare configuration complexity and performance metrics.

THEORY:

Static routing requires manual configuration for each route in a network, making it ideal for smaller setups. Dynamic routing protocols like RIP automatically adapt to topology changes, offering greater scalability.

Procedure:

1. Static Routing:
   - Configure three routers:
     - Router1 LAN: 192.168.1.0/24.
     - Router2 LAN: 192.168.2.0/24.
     - Router3 LAN: 192.168.3.0/24.
   - Establish WAN connections:
     - Router1 to Router2: 10.0.0.0/30.
     - Router2 to Router3: 10.0.0.4/30.
   - Add static routes on each router for inter-network communication.
2. Dynamic Routing (RIP):
   - Enable RIP protocol on all routers:
     - router rip → version 2.
   - Add connected networks under RIP configuration.

3. Testing and Comparison:
    - Test connectivity using ping.
    - Simulate link failure to analyze dynamic routing behavior.

Observations:

Static routing required manual updates for topology changes. RIP automatically adjusted routes, demonstrating higher adaptability.

Conclusion:

Dynamic routing protocols are preferred for larger, changing networks, while static routing is effective for simpler setups.

Experiment-9

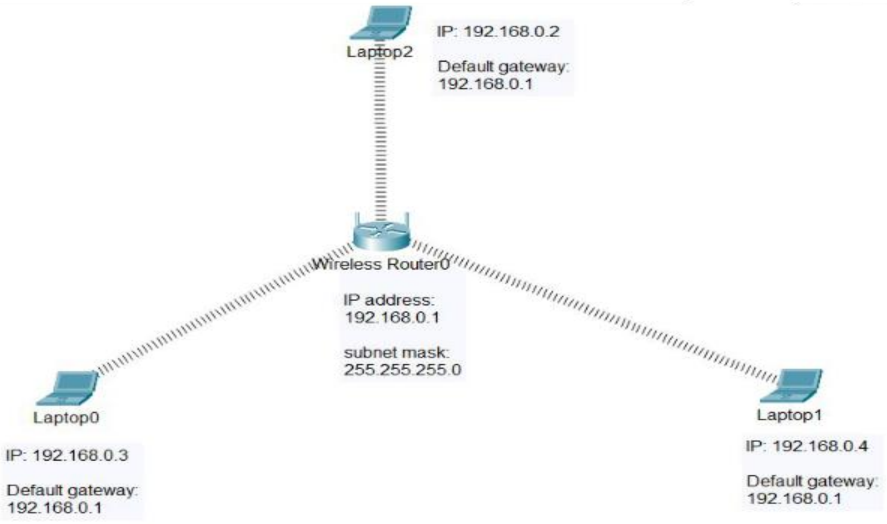
Aim: To configure WEP encryption on a wireless router and analyze its security limitations.

Apparatus:

Cisco Packet Tracer, wireless router, laptops, access points.

Objectives:

- Set up basic wireless router settings.
- Implement WEP encryption for network security.
- Test connection using proper and improper authentication.

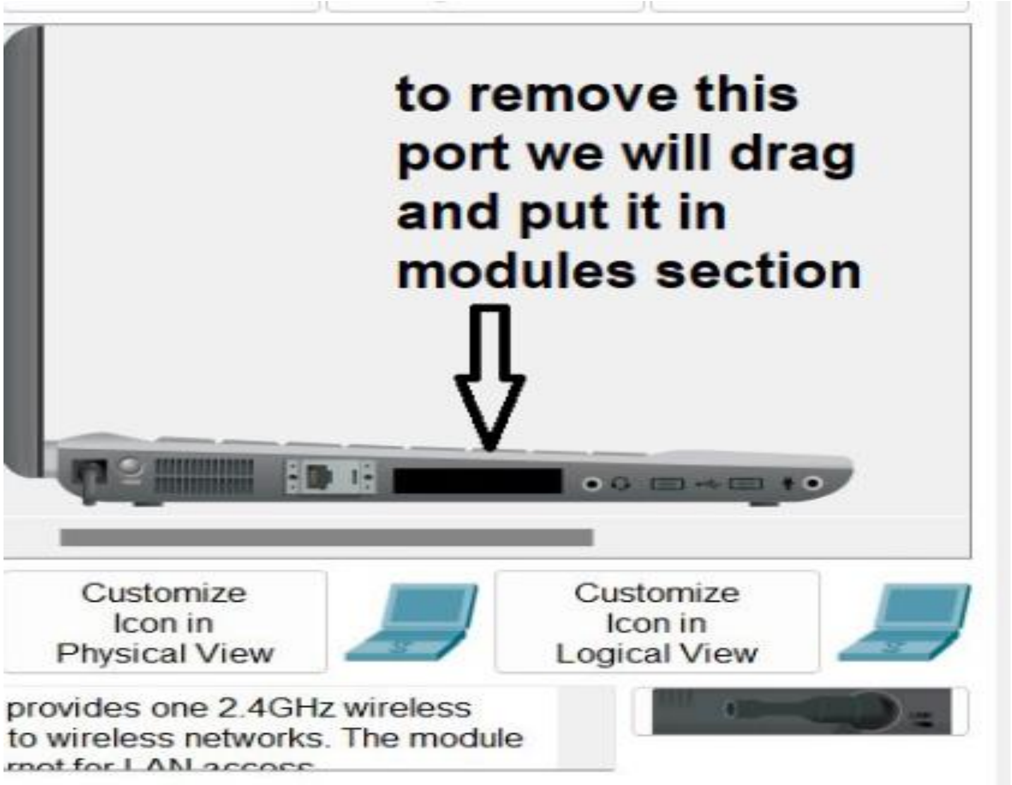

Laptop2
IP: 192.168.0.2
Default gateway: 192.168.0.1
Wireless Router0
IP address: 192.168.0.1
subnet mask: 255.255.255.0
Laptop0
IP: 192.168.0.3
Default gateway: 192.168.0.1
Laptop1
IP: 192.168.0.4
Default gateway: 192.168.0.1

THEORY:

WEP was an early wireless security protocol that used static encryption keys. Though once widely used, it is now considered insecure due to vulnerabilities in its encryption algorithms.

Procedure:

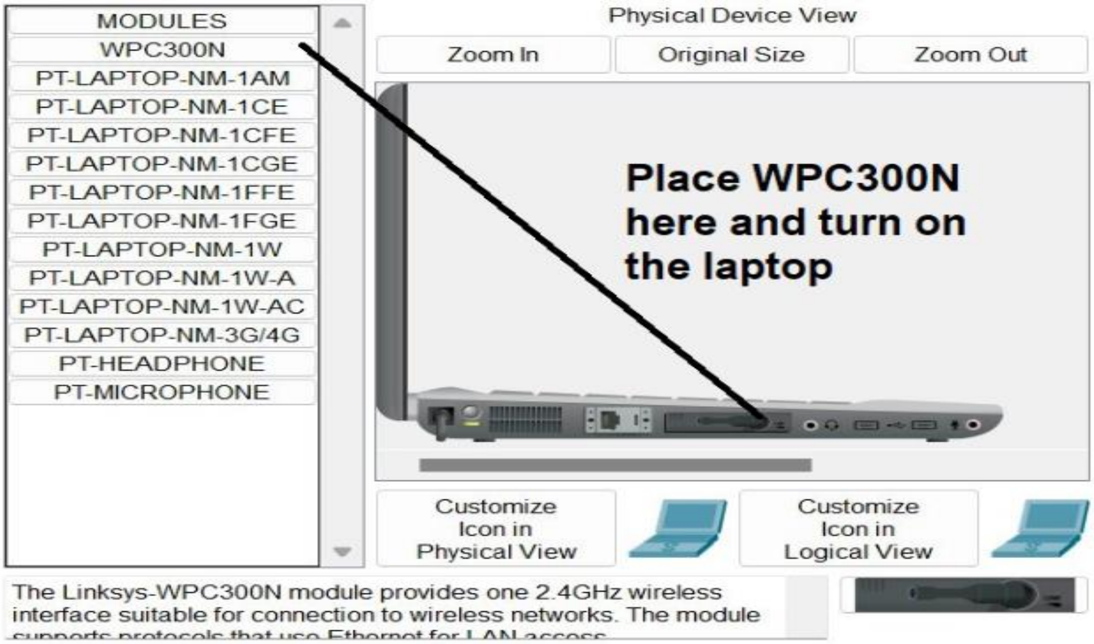
1. Router Configuration:
   - Assign LAN IP: 192.168.0.1/24.
   - Enable DHCP with range 192.168.0.100-150.
   - Configure SSID as "NetworkSecure".
   - Activate WEP encryption and set a key.
2. Client Configuration:



to remove this port we will drag and put it in modules section

Customize Icon in Physical View
Customize Icon in Logical View

provides one 2.4GHz wireless
to wireless networks. The module
rnot for LAN access



Place WPC300N here and turn on the laptop

The Linksys-WPC300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access

3. Testing and Observations:

   - Capture wireless traffic using tools (e.g., simulation or Wireshark).

   - Identify encrypted data patterns.

Observations:

WEP allowed connections only with the correct key, but vulnerabilities in its encryption were observed during traffic analysis.

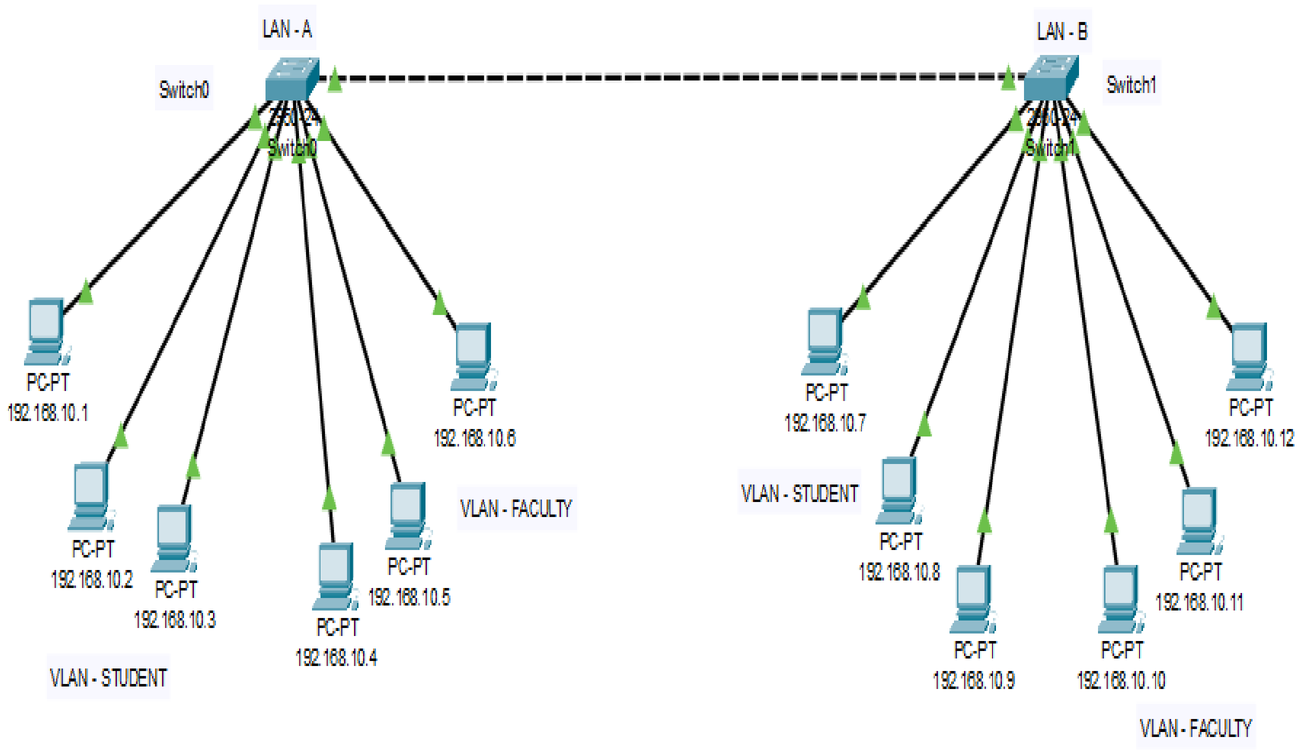
Conclusion:

WEP is outdated and insecure. Transitioning to WPA2 or WPA3 is recommended for modern networks.

Experiment-10

Aim: To configure intra-VLAN communication across multiple switches, ensuring seamless connectivity between devices in the same VLAN.

Apparatus: Cisco Packet Tracer, multiple switches, PCs, network cables.



Objectives:

- Create VLANs on switches.
- Configure trunk ports for inter-switch communication.
- Verify intra-VLAN connectivity.

THEORY:

VLANs segment network traffic logically, isolating groups of devices to improve performance and security. Trunk ports enable communication between VLANs across different switches.

Procedure:

1. **VLAN Creation:**

   Create VLANs on Switch1 and Switch2:

   - VLAN 10 (Office): 192.168.10.1

2. **CLI commands:**

```
Switch(config) #en
Switch(config) #vlan 2
Switch(config-vlan) #name office
Switch(config-vlan) #exit
Switch(config) #vlan 3
Switch(config-vlan) #name home
Switch (config-vlan)#exit
Switch(config) #interface fastethernet 0/1
Switch(config-if) #switchport access vlan 2
Switch(config-if) #exit
Switch(config)#interface fastethernet 0/2
Switch(config-if) #switchport access vlan 2
Switch(config-if) #exit
Switch(config) #interface fastethernet 0/3
Switch(config-if) #switchport access vlan 3
Switch(config-if) #exit
Switch(config) #interface fastethernet 0/4
Switch (config-if) #switchport access vlan 3
Switch(config-if) #exit
```

3. **Host Configuration:**

   - Assign IPs to PCs within VLAN 2,3

   - Connect PCs to access ports on Switch1 and Switch2.

Observations:

Devices in the same VLAN communicated seamlessly. Trunk ports ensured consistent traffic flow across switches.

Conclusion:

Intra-VLAN communication enhances network segmentation and performance.

Experiment-11

Aim: To enable and test Telnet access for remote router management, analyzing its security implications.

Apparatus: Cisco Packet Tracer, router, switch, PCs.

Objectives:

- Configure a router for Telnet access.
- Set up authentication for Telnet sessions.
- Understand Telnet's security risks.

THEORY:

Telnet allows remote management of network devices using plaintext communication. Though useful, it is insecure and has largely been replaced by SSH.

Procedure:

1. Router Configuration:

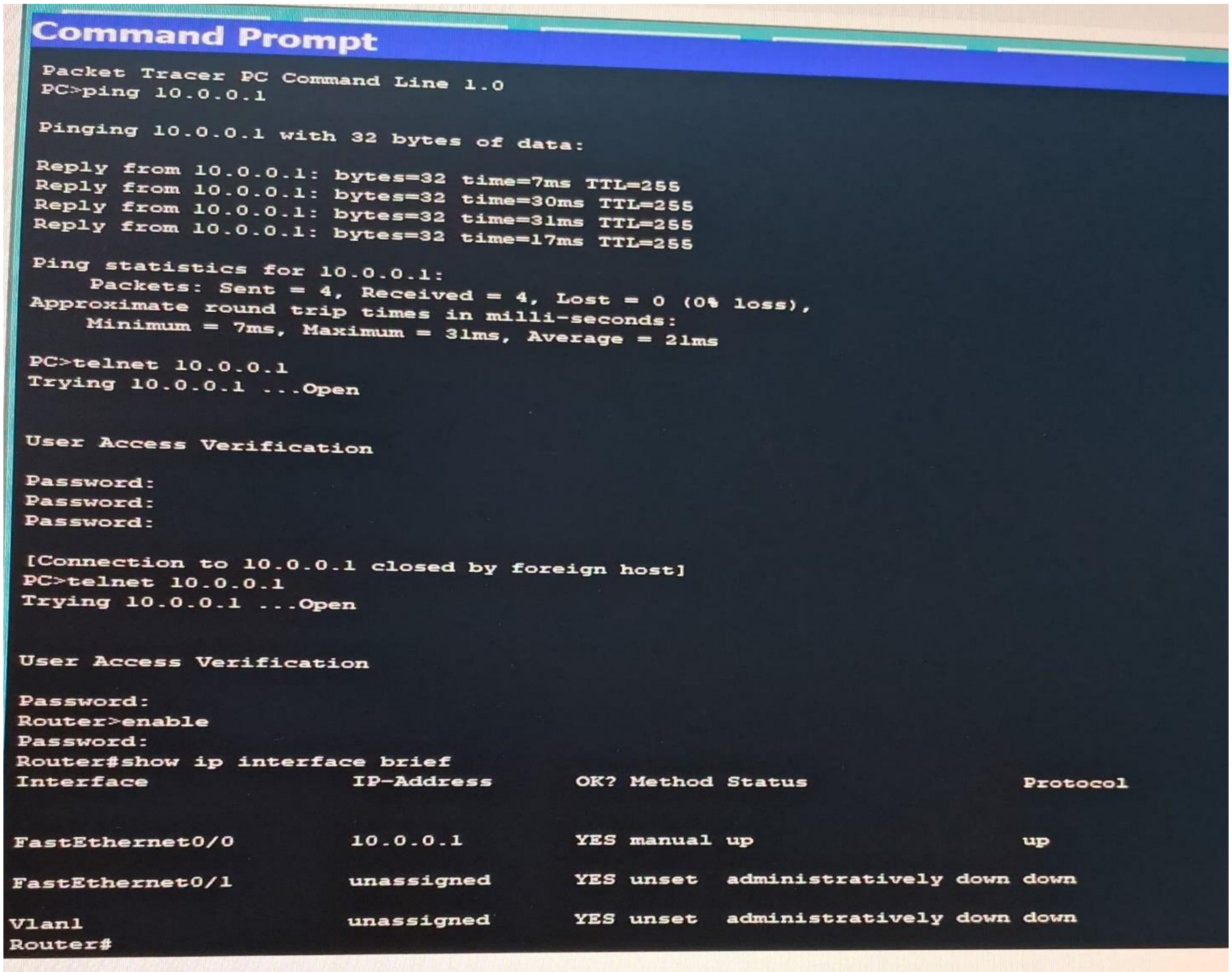
```
Router>en
Router#config t
Router (config)#interface fa0/0
Router(config-if)#ip address 10.0.0.1  255.0.0.0
Router (config-if) #no shut
Router(config-if) #line vty 0 4
Router(config-line) #password hello123
Router (config-line) #enable password pass123
```

2. Testing:

    - Test connectivity and execute basic commands remotely.
    - Analyze security risks using packet capture tools.

Observations:

Telnet transmitted data in plaintext, exposing passwords during packet capture.



```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=7ms TTL=255
Reply from 10.0.0.1: bytes=32 time=30ms TTL=255
Reply from 10.0.0.1: bytes=32 time=31ms TTL=255
Reply from 10.0.0.1: bytes=32 time=17ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 31ms, Average = 21ms

PC>telnet 10.0.0.1
Trying 10.0.0.1 ...Open


User Access Verification

Password:
Password:
Password:

[Connection to 10.0.0.1 closed by foreign host]
PC>telnet 10.0.0.1
Trying 10.0.0.1 ...Open


User Access Verification

Password:
Router>enable
Password:
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol


FastEthernet0/0        10.0.0.1        YES manual up                    up

FastEthernet0/1        unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
Router#
```

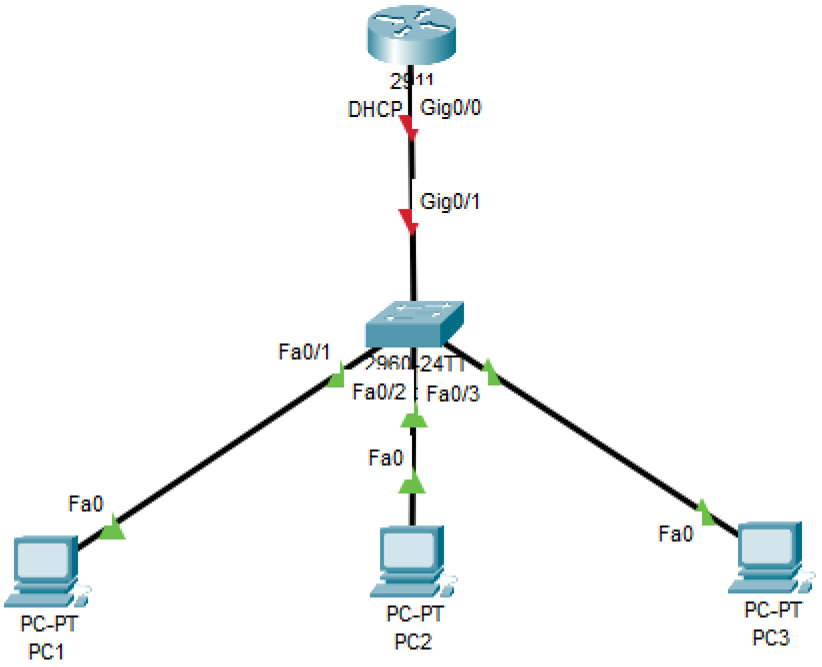
Conclusion:

Telnet is insecure for remote management; SSH should be used instead.

Experiment-12

Aim: To configure and test a DHCP server on a router for automatic IP assignment to clients.

Apparatus: Cisco Packet Tracer, router, switch, PCs.



Objectives:

- Configure a DHCP server on the router.
- Test automatic IP allocation to clients.
- Analyze DHCP message exchange.

THEORY:

DHCP automates IP assignment, reducing manual configuration efforts in networks. It is essential for managing large-scale setups efficiently.

Procedure:

1. Router Configuration:
   - Assign LAN IP: 192.168.1.1/24.
   - Exclude static IPs (e.g., 192.168.1.1-192.168.1.10).
   - Create a DHCP pool:
     - Network: 192.168.1.0/24.
     - Default gateway: 192.168.1.1.
2. Client Configuration:
   - Set PCs to “DHCP” mode.
   - Test IP assignment from the router.
3. Verification:
   - View DHCP bindings with show ip dhcp binding.
   - Test lease renewal and release.

Observations:

Clients received IPs automatically. DHCP improved efficiency compared to manual configuration.

Conclusion:

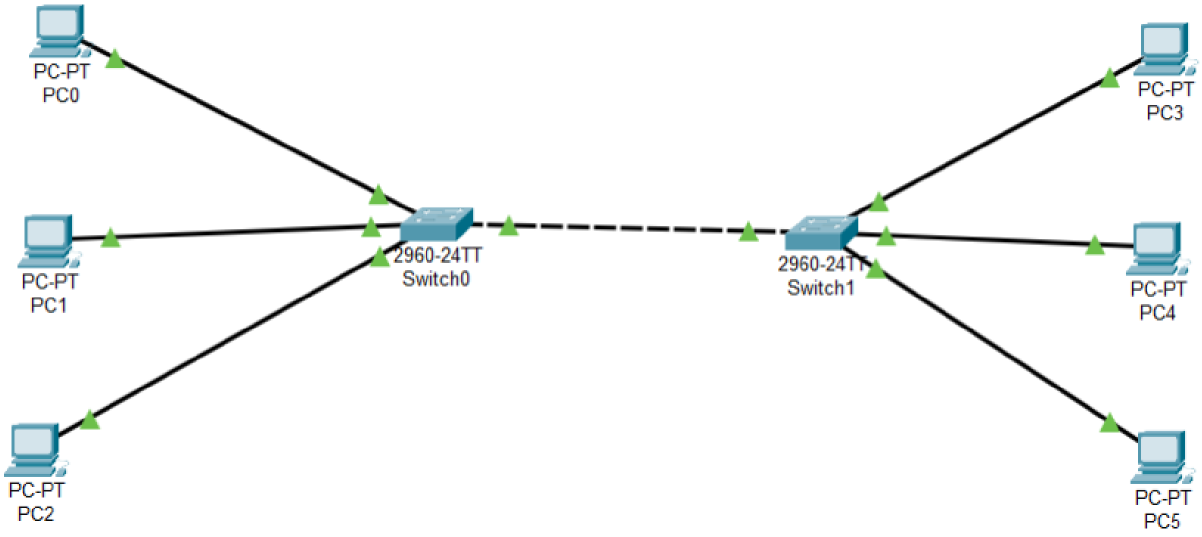
DHCP simplifies network management and ensures consistent IP allocation.

Experiment-13

Aim: To analyze data transmission between devices at different OSI layers, understanding the encapsulation and decapsulation process.

Apparatus:

Cisco Packet Tracer, two PCs, switch.



Objectives:

- Observe ARP resolution and MAC addressing.
- Analyze protocol headers added at each OSI layer.

THEORY:

Data transmission involves encapsulating packets at the sender and decapsulating them at the receiver. Protocols like ARP and TCP/IP ensure efficient communication.

Procedure:

1. Network Setup:
    - Connect two PCs through a switch.
    - Assign IPs (e.g., 192.168.1.10 and 192.168.1.20).
2. Testing:
    - Clear ARP cache (arp -d *).
    - Ping from PC1 to PC2.
    - Capture traffic using tools to analyze protocol headers.

Observations:

- ARP resolved IP to MAC addresses.
- ICMP packets showed encapsulation at each OSI layer.

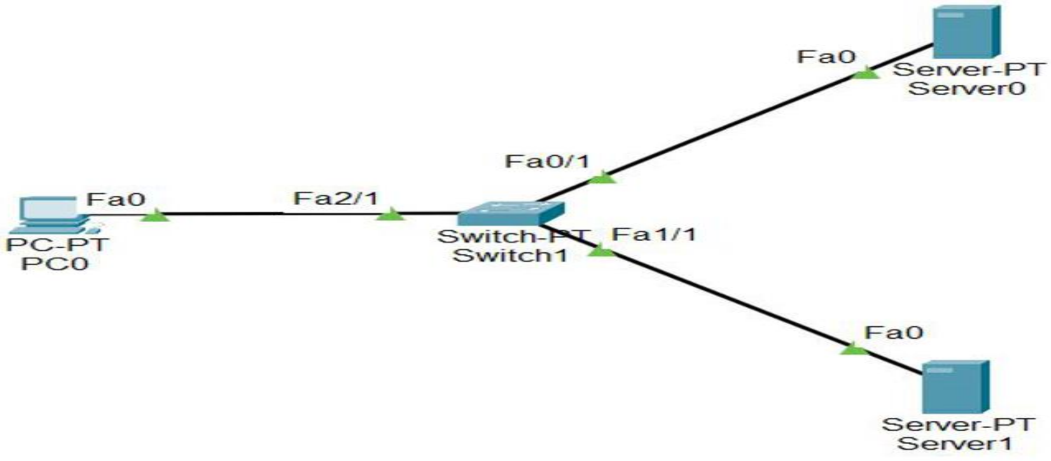
Conclusion:

Data transmission involves multiple layers and protocols working together.

Experiment-14

Aim: To configure and test a DNS server for translating domain names to IP addresses.

Apparatus: Cisco Packet Tracer, DNS server, router, PCs.



THEORY:

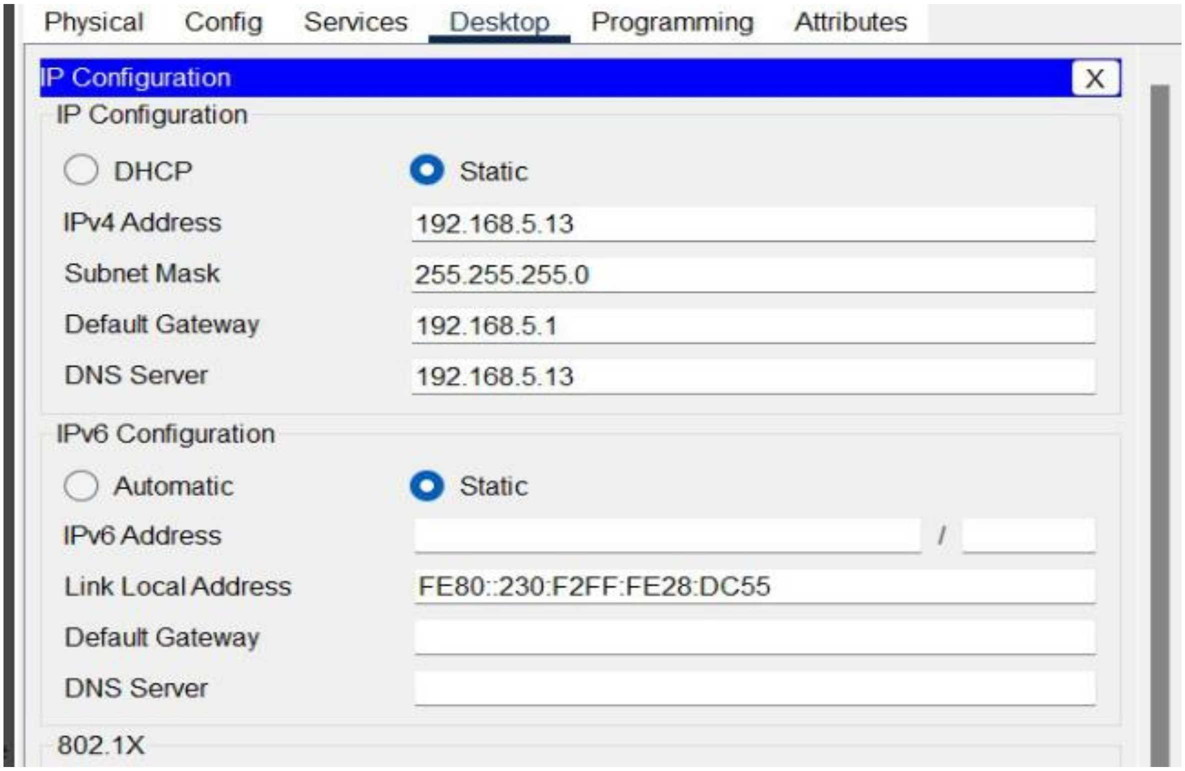
DNS simplifies network access by translating human-readable names into IP addresses.

Procedure:

Step 1: First, open the cisco packet tracer desktop and select the devices given below:

S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway	DNS
1.	PC0	192.168.5.11	255.255.255.0	192.168.5.1	nil
2.	server0	192.168.5.12	255.255.255.0	192.168.5.1	nil
3.	DNS	192.168.5.13	255.255.255.0	192.168.5.1	192.168.5.13

Step 2: Configure the PCs (hosts) Server0 and DNS with IPv4 address and Subnet Mask according to the IP addressing table given above.



IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.5.13

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.5.1

DNS Server: 192.168.5.13

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::230:F2FF:FE28:DC55

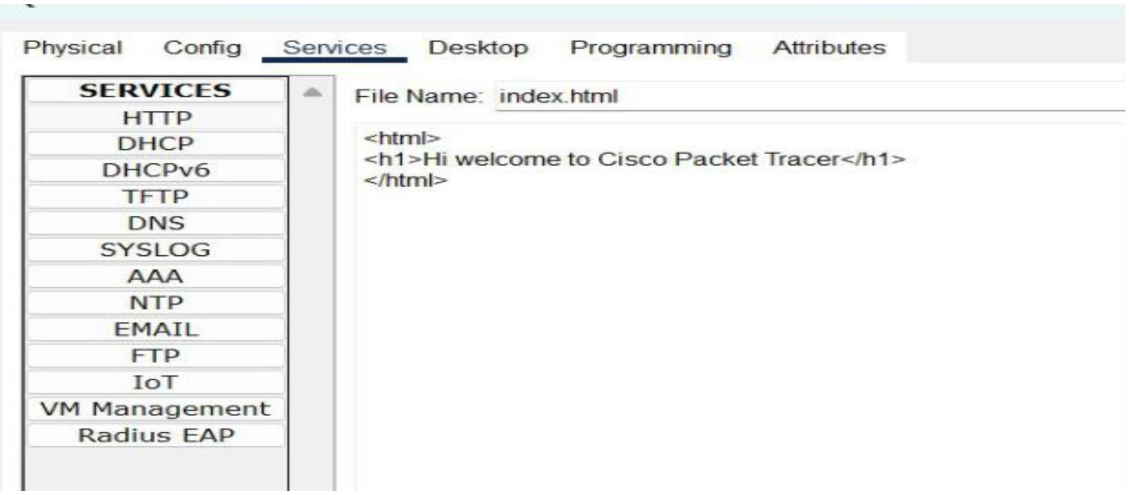
Default Gateway:

DNS Server:

802.1X

Step 3: Configure the HTTP sever 0

- To configure the HTTP server.
- Go to services then click on HTTP
- Then delete all of the files except the index.html and edit it.

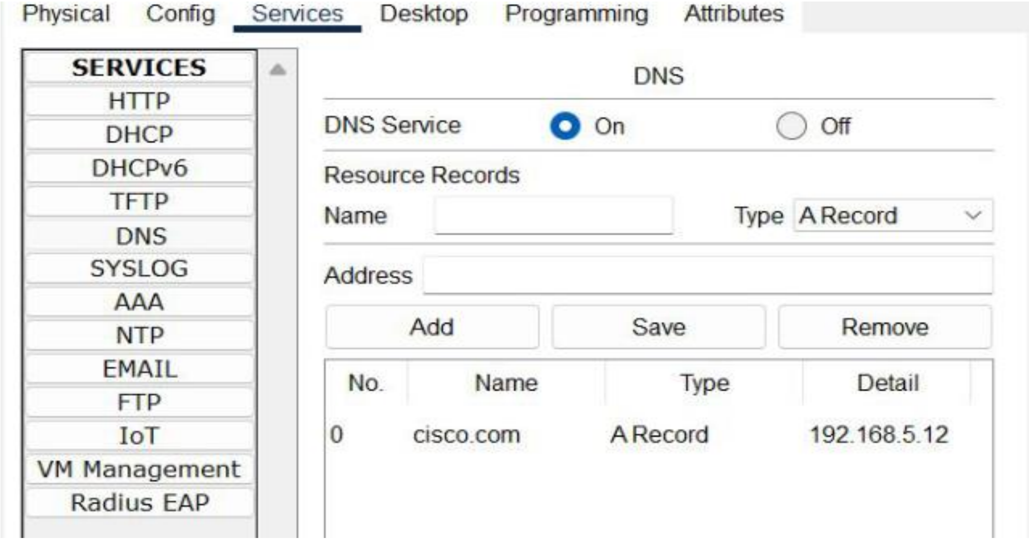


File Name: index.html

```
<html>
<h1>Hi welcome to Cisco Packet Tracer</h1>
</html>
```

Step 4: Configure the DNS server

- To configure the DNS server.
- Go to services then click on DNS.
- Then turn on the DNS services.
- Name the server cisco.com and type address 192.168.5.12
- And add the record.



DNS

DNS Service ● On ○ Off

Resource Records

Name

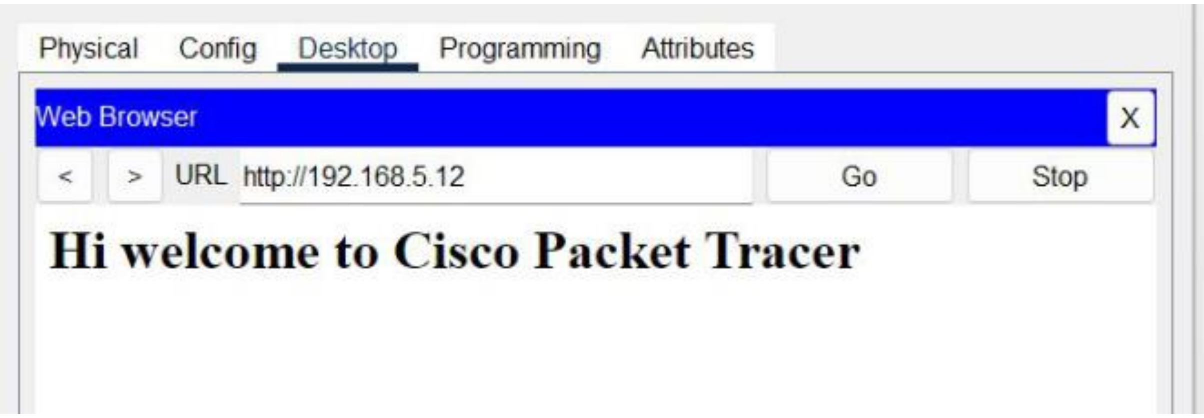
Type A Record

Address

No.	Name	Type	Detail
0	cisco.com	A Record	192.168.5.12

Step 5: Verify the server by using the web browser in the Host.

- Enter the IP address of server0 and click on GO.
- It will show the results.



URL http://192.168.5.12

Hi welcome to Cisco Packet Tracer