

Experiment Number: 01

Name of the Experiment: Configure Local Area Network LAN (Wired).

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Switch.
 2. UTP Cable (Straight Through).
 3. End Devices (Desktop, Laptop).
 4. IP Address (192.168.0.1)

Description: A wired Local Area Network (LAN) connects computers and devices using physical cables, typically Ethernet cables. These cables run from each device to a central device like a switch or router, which helps manage the network traffic.

Wired LANs are known for being faster and more stable than wireless networks because they are less affected by interference or signal drops. They are often used in places where reliability is essential, such as offices, schools, or gaming setups. However, the main limitation is that devices need to stay connected by cables, which can make it harder to move them around freely.

Configuration Procedure:

To Configure of Local Area Network LAN (Wired) we have to follow the following steps:

1. First, we have to drag and drop a switch onto the Cisco Packet Tracer interface.
2. Next, we select some end devices such as Laptops and Desktops that support NIC cards with RJ45 connectors.
3. Then, we choose a copper "Straight-Through" UTP cable to connect the devices.
4. We click on the switch and select a specific port for the new connection.
5. We repeat the process of selecting switch ports until all end devices are connected.
6. We double-click on an end device, and by default, the interface opens on the "Physical" tab.
7. Then, we switch to the "Desktop" tab and click on "IP Configuration."
8. We enter the IP address (192.168.0.1), and the subnet mask fills in automatically after clicking submit.
9. After that, we close the configuration section.
10. Finally, we assign IP addresses to all remaining end devices following the same steps.

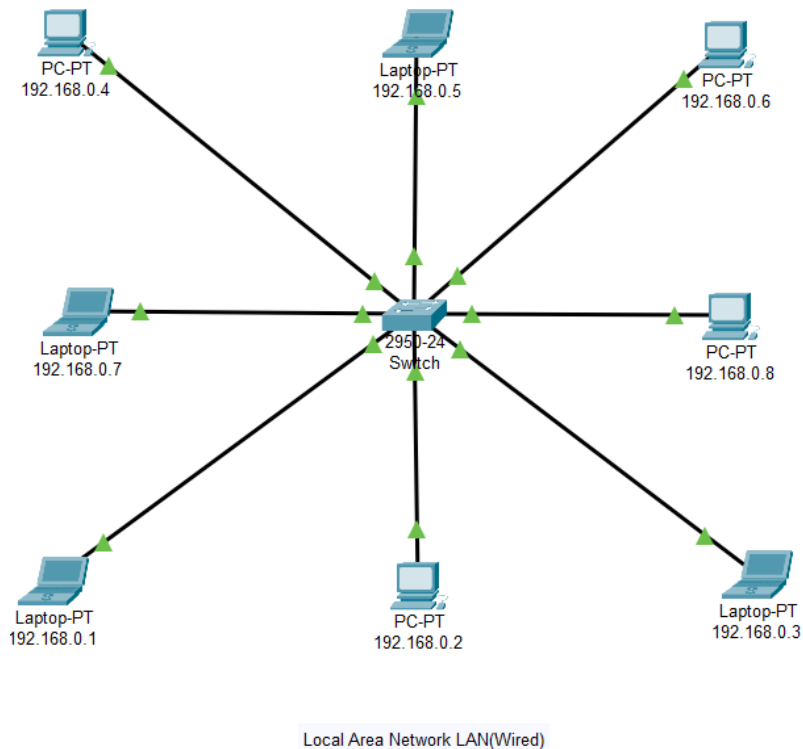


Figure 01: Configuration of Local Area Network LAN (Wired).

Simulation Process:

- **Method 1**

1. First, we have to select a packet from the top sidebar. The mouse pointer will change to a packet symbol.
2. Next, we select the first PC and then another PC using the packet symbol pointer.
3. This action indicates that the packet will flow from the first device to the second device.
4. Finally, we can see a success notification in the bottom-right section of the screen.

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|------|-------------|-------------|-------------|------|-------|-----------|----------|-----|------------------------|
| | Successful | 192.168.0.4 | 192.168.0.3 | ICMP | | 0.000 | N | 0 | (edit) |
| | Successful | 192.168.0.6 | 192.168.0.1 | ICMP | | 0.000 | N | 1 | (edit) |
| | Successful | 192.168.0.5 | 192.168.0.8 | ICMP | | 0.000 | N | 2 | (edit) |
| | Successful | 192.168.0.2 | 192.168.0.7 | ICMP | | 0.000 | N | 3 | (edit) |

Figure 02: Simulation using the first method.

- **Method 2:**

1. First, we have to double-click on the PC and select the "Desktop" tab.
2. Next, we click on "Command Prompt."
3. For example, if the PC has the IP address 192.168.0.1, we will ping 192.168.0.6.
4. We type "ping 192.168.0.6" and press Enter.

5. If the physical and logical connections are correct, the result will show:
Packet Sent = 4, Packet Received = 4, Packet Lost = 0%.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.6

Pinging 192.168.0.6 with 32 bytes of data:

Reply from 192.168.0.6: bytes=32 time<1ms TTL=128
Reply from 192.168.0.6: bytes=32 time<1ms TTL=128
Reply from 192.168.0.6: bytes=32 time<1ms TTL=128
Reply from 192.168.0.6: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Figure 03: Simulation using the second method.

Results and Discussions: Both methods were executed successfully, confirming that the connections between devices functioned as intended. The successful packet transfer and the successful ping results demonstrate that the experiment was effective. Therefore, we can conclude that the experiment was successful.

Precautions:

1. We must select "Static" when configuring the IP address and input each IP address manually.
2. Each device should have an IP address that belongs to the same network; if we select an IP address from a different network, the devices will not be able to communicate effectively.

Experiment Number: 02

Name of the Experiment: Configure Local Area Network LAN (Wireless).

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Router (Linksys-WRT300N).
 2. End Devices (Desktop, Laptop, Smart phones and Tablets).
 3. IP Address (192.168.1.1)

Description: A wireless Local Area Network (WLAN) connects devices like computers, smartphones, and printers using Wi-Fi instead of physical cables. In a WLAN, devices communicate with a central device called a router or access point, which sends and receives data over radio signals.

Wireless LANs are convenient because they allow users to connect from anywhere within the signal range, giving more flexibility to move devices around. However, they can sometimes be slower than wired networks and are more prone to interference from walls, other electronic devices, or network congestion. Security is also a concern, so encryption methods like WPA2 or WPA3 are used to keep the network safe.

Configuration Procedure:

To Configure of Local Area Network LAN (Wireless) we have to follow the following steps:

1. First, we drag and drop a wireless router and some devices that support wireless communication onto the Cisco Packet Tracer interface.
2. For the desktop PC, we double-click on the PC-PT, which opens on the "Physical" tab by default. First, we power off the PC. Then, we need to add the "Linksys-WMP300N" module to this PC.
3. We replace the existing module with the "Linksys-WMP300N" module.
4. After that, we power on the device.

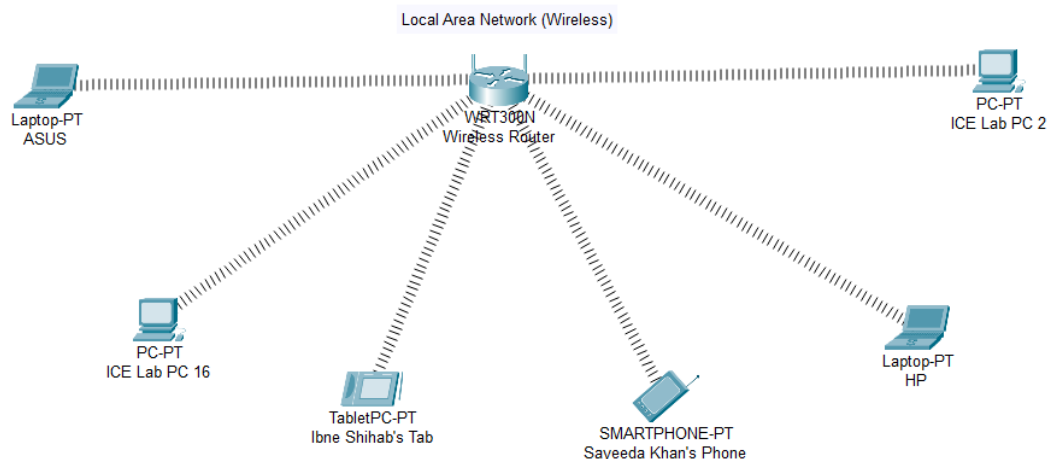


Figure 01: Configuration of Local Area Network LAN (Wireless).

5. The same procedure applies for the laptop. Now both the desktop and laptop are ready to communicate over wireless media.

Router Configuration:

1. For the router configuration, we double-click on the router and go to the “Config” tab. Then, we select the “Wireless” option.
2. Next, we give a name to our access point (SSID).
3. We then choose an authentication type. By default, it is set to "Disabled," so we select “WPA-PSK” and set the password to 123454678, then close the configuration.
4. We double-click on the desktop PC and open “PC Wireless” from the “Desktop” tab.
5. In the “Connect” tab, which shows link information by default, we press the “Refresh” button.
6. After refreshing, we should see our access point; we then press the “Connect” button.
7. We enter the network password in the “Pre-Shared Key” field and then click “Connect.” We repeat the same steps on the laptop.

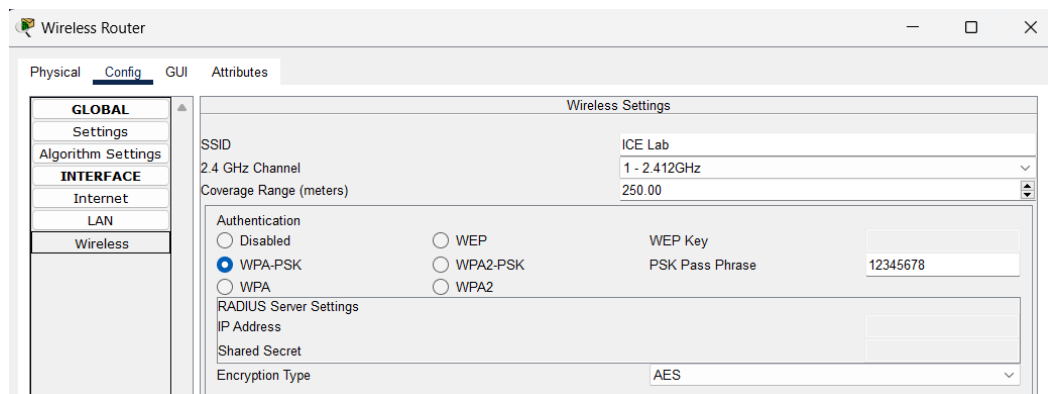


Figure 02: Configuration of the Router.

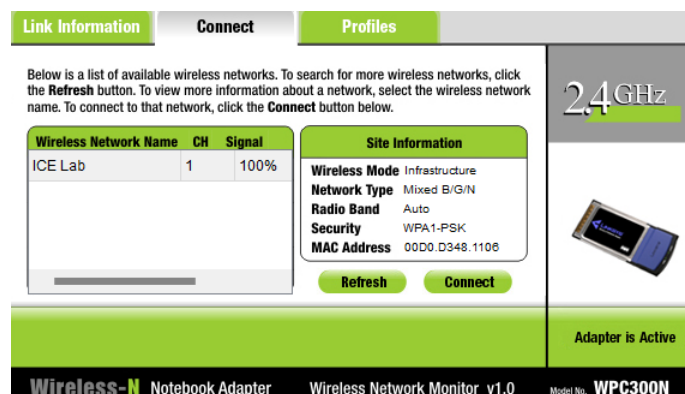


Figure 03: Connection configuration of Local Area Network LAN (Wireless).

Configure For PDA:

1. For the PDA configuration, we double-click on the PDA and select the “Config” tab, then choose “Wireless” from the bottom left.
2. We enter the access point name (SSID) and the password as “WPA-PSK,” then close the configuration.
3. We repeat the same steps for the tablet.

Simulation Process:

• Method 1

1. We select a packet from the right sidebar, and the mouse pointer changes to a packet symbol.
2. Next, we select the first PC and then select another PC using the packet symbol pointer.
3. This action indicates that a packet will flow from the first device to the second device.
4. We can then see a successful notification in the bottom-right section.









| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|---|-------------|----------------------|----------------------|------|--|-----------|----------|-----|--------|
|  | Successful | ASUS | HP | ICMP |  | 0.000 | N | 0 | (edit) |
|  | Successful | ICE Lab PC 2 | ICE Lab PC 16 | ICMP |  | 0.000 | N | 1 | (edit) |
|  | Successful | Ibne Shihab's Tab | Sayeeda Khan's Phone | ICMP |  | 0.000 | N | 2 | (edit) |
|  | Successful | Sayeeda Khan's Phone | Ibne Shihab's Tab | ICMP |  | 0.000 | N | 3 | (edit) |

Figure 04: Simulation using the first method.

• Method 2

1. We double-click on a PC, select the “Desktop” tab, and click on “Command Prompt.”
2. For example, if this PC has the IP address 192.168.0.104, we will ping 192.168.0.100.
3. We type “ping 192.168.0.100” and press Enter.
4. If the physical and logical connections are correct, the result will show:
Packet Sent = 4, Packet Received = 4, Packet Lost = 0%.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=42ms TTL=128
Reply from 192.168.0.100: bytes=32 time=18ms TTL=128
Reply from 192.168.0.100: bytes=32 time=12ms TTL=128
Reply from 192.168.0.100: bytes=32 time=20ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 42ms, Average = 23ms
```

Figure 05: Simulation using the second method.

- **Method 3**

1. We double-click on the desktop or laptop, then select “Web Browser” from the “Desktop” tab.
2. We enter the router's IP address in the browser's address bar and press Enter.
3. A command prompt will appear for authentication, where we enter the username and password as "admin."
4. If everything is correct, we will be granted access to the router.

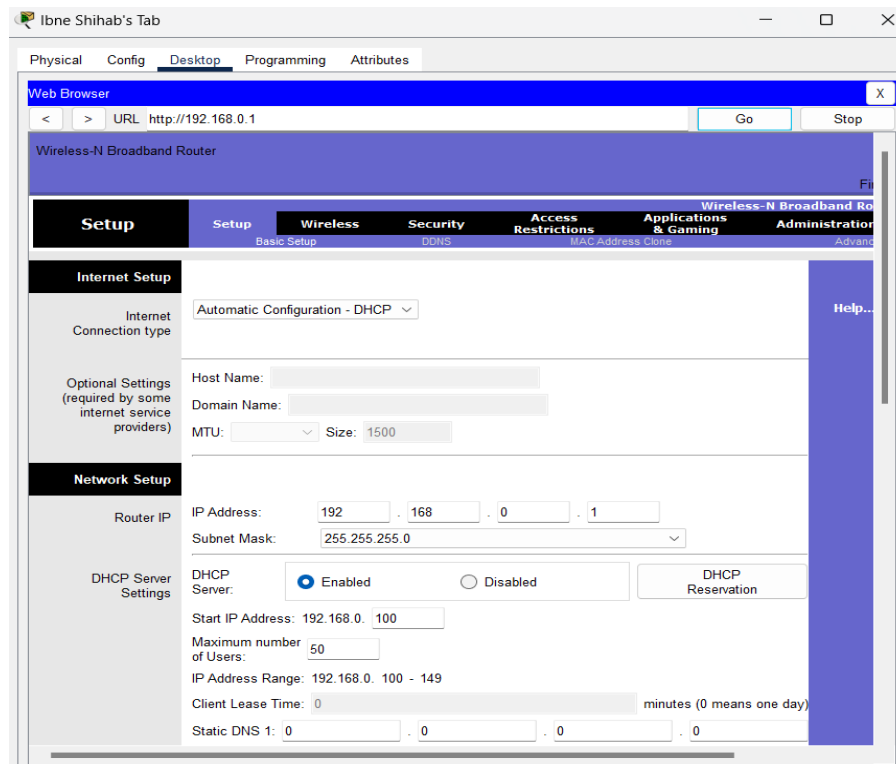


Figure 06: Simulation using the third method.

Results and Discussion: The experiment successfully established a wireless network using a router and various end devices.

1. Successful packet transfer between PCs confirmed proper network connections.
2. Ping Test: All packets were sent and received without loss, demonstrating reliable communication.
3. Router Access: Successful login to the router's control panel verified correct configuration.

Precautions

1. Ensure correct IP addressing within the same subnet.
2. Position the router centrally for better coverage.
3. Verify device compatibility with wireless standards.
4. Monitor network performance regularly.

Experiment Number: 03

Name of the Experiment: Transferring packets through two different networks.

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Switch.
 2. UTP Cable (Straight Through).
 3. End Devices (Desktop, Laptop).
 4. IP Address (192.168.1.1 & 192.168.2.1)
 5. Router.

Description: Transferring packets through two different networks involves the process of routing data from one network to another. When a device wants to communicate with another device on a different network, it sends a packet containing the source and destination IP addresses. The packet first reaches a local router, which determines the best path for the packet based on its destination address.

The router checks its routing table to decide where to forward the packet next, potentially sending it through multiple routers across different networks. Each router it passes through may encapsulate the packet in different link layer protocols suitable for the next segment of the journey.

Once the packet reaches the destination network, the router uses the Address Resolution Protocol (ARP) to find the MAC address of the target device. The packet is then delivered to the intended device, which processes the data. This process allows for seamless communication between devices on separate networks, relying on the routing capabilities of routers and proper IP addressing.

Configuration Procedure:

1. Placed Components:

- We dragged and dropped **two switches** (2960-24 as Switch1 and Switch2), **one router** (1841 Router), and several **end devices** (PCs and Laptops) onto the Cisco Packet Tracer workspace.

2. Connected the Devices:

- We used the appropriate cables to **connect the router** to both switches:
 - Router's **Fast Ethernet 0/0** was connected to **Switch1**.
 - Router's **Fast Ethernet 0/1** was connected to **Switch2**.
- Then, we connected the **end devices** to the switches:
 - End devices with IPs in the range 192.168.1.x were connected to **Switch1** (Network 1).

- End devices with IPs in the range 192.168.2.x were connected to **Switch2** (Network 2).

3. **Configured the Router Interfaces:**

- We double-clicked the router and accessed the **CLI**, typing no when prompted about system maintenance.

4. **Entered Privilege Mode:**

- We typed enable to enter privilege mode.

5. **Configured the First Interface (fa 0/0):**

- In privilege mode, we entered **global configuration mode** by typing configure terminal.
- We typed interface fa0/0 to access **Fast Ethernet 0/0**, which was connected to **Switch1**.
- We then assigned the IP address and subnet mask for **Network 1**: ip address 192.168.1.1 255.255.255.0.
- The interface was activated by typing no shutdown.

6. **Configured the Second Interface (fa 0/1):**

- After exiting the current interface configuration by typing exit, we typed interface fa0/1 to access **Fast Ethernet 0/1**, which was connected to **Switch2**.
- We assigned the IP address and subnet mask for **Network 2**: ip address 192.168.2.1 255.255.255.0.
- The interface was then activated with no shutdown.

7. **Saved the Configuration:**

- We exited the interface configuration, returned to privilege mode by typing exit, and saved the configuration by typing wr.

8. **Assigned IP Addresses to End Devices:**

- For each PC and Laptop connected to **Switch1**, we assigned IP addresses in the range 192.168.1.x (e.g., 192.168.1.2, 192.168.1.3, etc.).
- For each PC and Laptop connected to **Switch2**, we assigned IP addresses in the range 192.168.2.x (e.g., 192.168.2.2, 192.168.2.3, etc.).

9. **Set Gateway on Each Device:**

- On devices connected to **Network 1**, we set the default gateway to 192.168.1.1.
- On devices connected to **Network 2**, we set the default gateway to 192.168.2.1.

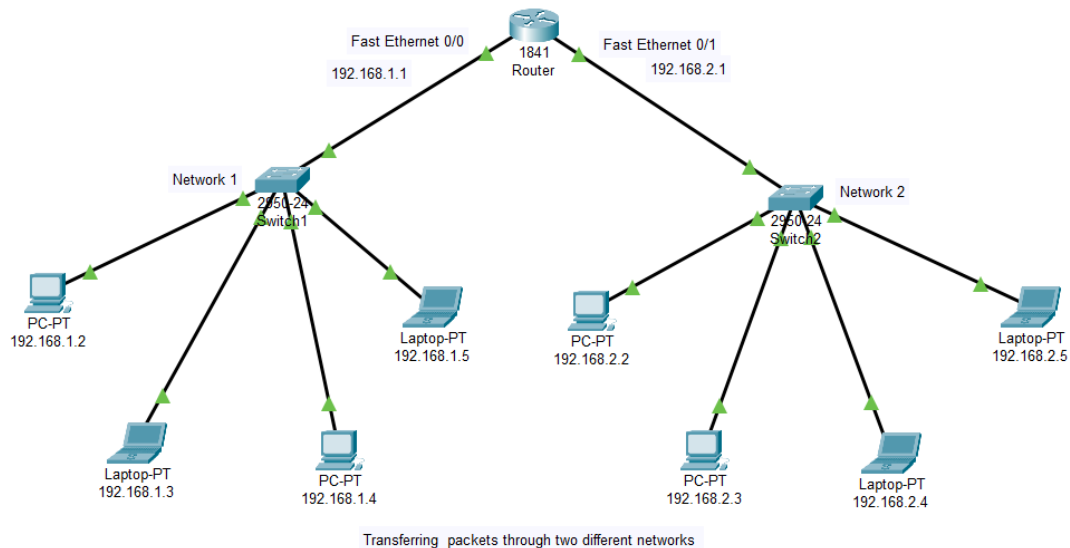


Figure 01: Transferring packets through two different networks.

CLI Command:

```

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!

Router>enable

Router#config t

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 shut

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

Router(config)#int fa 0/1

Router(config-if)#ip address 192.168.2.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit

Router(config)#exit

Router#

%SYS-5-CONFIG_I: Configured from console by console

```

```
Router#wr
Building configuration...
[OK]
Router#
Router con0 is now available
```

Simulation Process:

- **First Way: Packet Transfer Using the Packet Symbol**
 1. A packet is selected from the right sidebar, changing the mouse pointer to a packet symbol.
 2. The first PC is chosen, followed by another PC using the packet symbol pointer.
 3. This action indicates that a packet will flow from the first device to the second device.
 4. A successful notification appears in the bottom-right section.
- **Second Way: Using Command Prompt for Ping Test**
 1. The PC is double-clicked to open, and the “Desktop” tab is selected, followed by clicking on “Command Prompt.”
 2. If this PC has the IP address 192.168.1.1, we ping the address 192.168.1.2.
 3. The command “ping 192.168.1.2” is typed, and Enter is pressed.
 4. If the physical and logical connections are correct, the result will display:
Packet Sent = 4, Packet Received = 4, Packet Lost = 0%.







| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|---|-------------|-------------|-------------|------|---|-----------|----------|-----|--------|
|  | Successful | 192.168.1.2 | 192.168.2.2 | ICMP |  | 0.000 | N | 0 | (edit) |
|  | Successful | 192.168.2.5 | 192.168.1.5 | ICMP |  | 0.000 | N | 1 | (edit) |
|  | Successful | 192.168.2.3 | 192.168.1.3 | ICMP |  | 0.000 | N | 2 | (edit) |

Figure 02: Simulation process using the packet symbol.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=6ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Figure 03: Simulation process using the ping test.

Results and Discussions: The experiment showed that packets were successfully transferred between two different networks.

1. **First Method:** Using the packet symbol, we confirmed that a packet moved from one PC to another, indicated by a success notification. This means the devices were connected correctly.
2. **Second Method:** The ping test showed **4 packets sent, 4 packets received, and 0 packets lost**. This result confirms that the devices could communicate without any issues.

Overall, the experiment proved that the network setup worked well, allowing devices to send and receive data.

Precautions

1. **Check IP Addresses:** Ensure all devices have the correct IP addresses for their networks (e.g., 192.168.1.x for Network 1 and 192.168.2.x for Network 2).
2. **Set Default Gateways:** Make sure the default gateway is configured correctly on each device (e.g., 192.168.1.1 for Network 1 and 192.168.2.1 for Network 2).
3. **Verify Configuration:** Ensure the router settings are correct.
4. **Inspect Connections:** Check that all cables are securely connected.

Experiment Number: 04

Name of the Experiment: Dynamic IP through Dynamic Host Configuration Protocol (DHCP).

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Switch.
 2. UTP Cable (Straight Through).
 3. End Devices (Desktop, Laptop).
 4. IP Address (192.168.1.1)
 5. Router.

Description: DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP addresses and other network configuration settings to devices on a network. This helps simplify network management by eliminating the need for manual IP address configuration. Key Features of DHCP:

1. Automatic IP Address Assignment: When a device connects to the network, it requests an IP address from a DHCP server, which assigns one from a predefined range.
2. Centralized Management: Network administrators can manage IP addresses from a single DHCP server, making it easier to handle network changes.
3. Efficient Address Use: DHCP can recycle IP addresses, allowing devices to share addresses temporarily rather than permanently using them.
4. Configuration Settings: In addition to IP addresses, DHCP provides devices with essential settings, such as subnet masks, default gateways, and DNS server addresses.

Overall, DHCP streamlines the process of connecting devices to a network, ensuring they can communicate effectively and efficiently.

Configuration Procedure:

1. **Placed Components:** We dragged and dropped **one switch, one router, and an end device** onto the Cisco Packet Tracer workspace.
2. **Connected the Devices:** We used a **UTP Straight Through Cable** to connect the router to the switch.
3. **Accessed the Router:** We double-clicked on the router and selected the **CLI Mode**.
4. **Entered Privilege Mode:** We typed enable to enter privilege mode.
5. **Accessed Interface:** We entered **global configuration mode** by typing configure terminal and accessed the interface by typing interface fa0/0.

6. **Assigned IP and Subnet Mask:** We assigned the IP address and subnet mask, then typed `no shutdown` to activate the interface.
7. **Exited to Global Configuration:** We typed `exit` to return to global configuration mode.
8. **Created DHCP Pool:** We typed `ip dhcp pool myPoolName` to create a DHCP pool.
9. **Configured Network and Default IP:** We specified the network and the router's default IP address for the DHCP pool.
10. **Saved Changes:** We typed `exit` to leave the DHCP configuration and saved the changes.
11. **Configured the End Device:** We double-clicked on the end device, selected the **Desktop** tab, and clicked on **IP Configuration**.
12. **Requested IP Address:** We selected **DHCP** to send a request for an IP address.

This process successfully set up a DHCP server on the router, allowing the end device to automatically obtain an IP address.

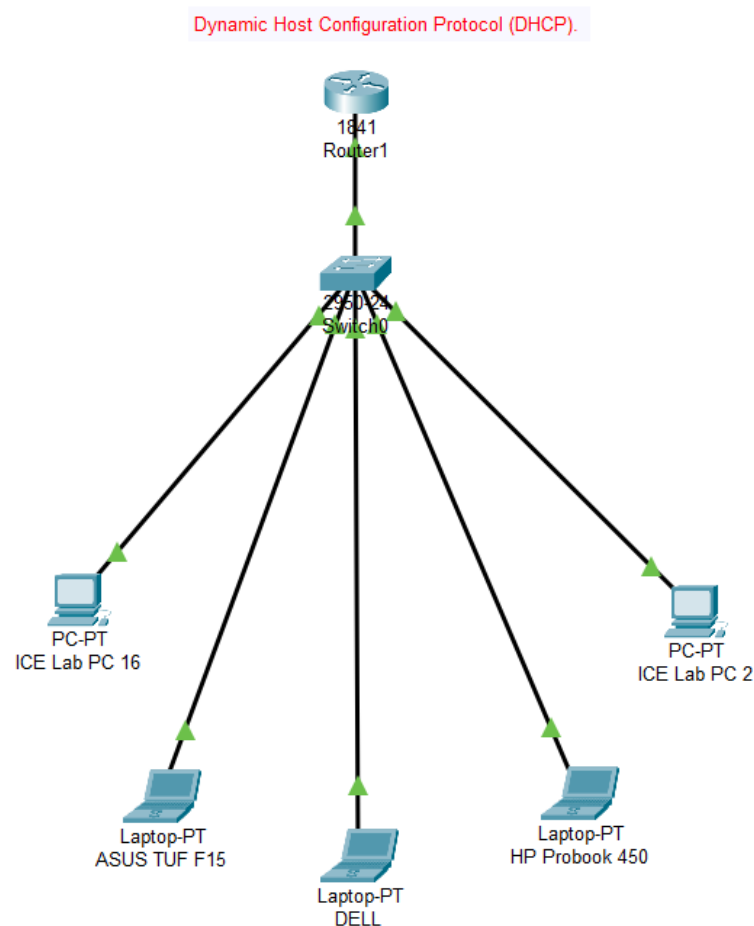


Figure 01: Configuration of Dynamic IP through Dynamic Host Configuration Protocol (DHCP).

CLI Command:

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#
Router(config-if)#exit
Router(config)#ip dhcp pool shihab
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...

[OK]
Router#
Router con0 is now available
```

Simulation Process:

If we go to the **Desktop** section of the end devices and select **IP Configuration**, choosing the **DHCP** option allows the device to automatically receive an IP address, subnet mask, default gateway, and DNS settings from the DHCP server. There is no need to manually assign these values, as the router provides them automatically. This simplifies network configuration and ensures seamless communication between devices.

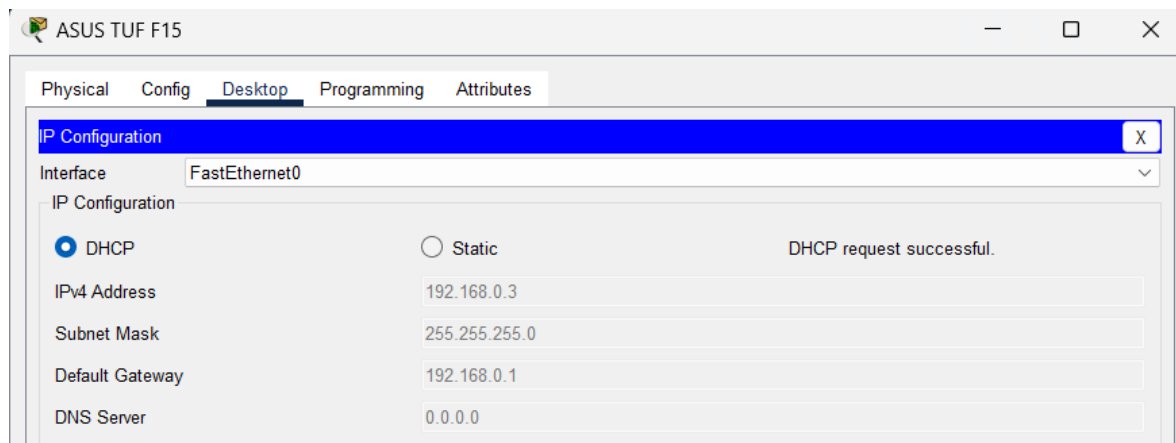


Figure 02: DHCP request successful.

Results and Discussion: The DHCP configuration was successfully implemented. When the end devices were set to **DHCP** mode, they automatically received IP addresses along with the subnet mask and gateway information from the router. This confirmed that the router was functioning correctly as a DHCP server, streamlining the IP assignment process and avoiding manual configurations. The network devices could communicate efficiently without IP conflicts or connection issues.

Precautions:

1. Ensure that the **DHCP pool** matches the network's IP range to prevent addressing errors.
2. The **default gateway IP** (e.g., 192.168.0.1) must be correctly assigned on the router to allow communication between devices.
3. Each network should have **unique IP ranges** to avoid conflicts if multiple networks are connected.
4. Use **UTP Straight Through Cables** for proper connections between devices and switches/routers.

Experiment Number: 05

Name of the Experiment: Configure Routing Information Protocol (RIP).

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Switch.
 2. UTP Cable (Straight Through).
 3. End Devices (Desktop, Laptop).
 4. IP Address (192.168.1.x, 192.168.2.x & 192.168.3.x)
 5. Router.
 6. Copper crossover cable.

Description: RIP (Routing Information Protocol) is a dynamic routing protocol used to help routers exchange information about networks. It determines the best path to a destination based on the number of hops (steps) between routers, with a maximum limit of 15 hops to prevent routing loops. RIP periodically updates routing tables, ensuring routers have up-to-date path information. Version 2 (RIP v2) supports classless routing, allowing the use of subnet masks, which makes it more flexible than the earlier version. Though simple to configure, RIP is best suited for smaller networks due to its limitations in scalability and efficiency compared to more advanced protocols.

Procedure for RIP Configuration:

1. Placed Devices:
 - We dragged and dropped routers, switches, and PCs onto the Cisco Packet Tracer workspace.
2. Connected Devices:
 - We connected the PCs to switches and the switches to routers using UTP Straight Through Cables.
 - Routers were interconnected using serial or cross-over cables where needed.
3. Accessed Router CLI:
 - We double-clicked the router, went to the CLI Tab, and typed:
 - enable to enter privileged mode.
 - configure terminal to enter global configuration mode.
4. Assigned IP Addresses to Interfaces:
 - For each interface, we entered:
 - interface fa0/0
 - ip address 192.168.1.1 255.255.255.0

- no shutdown
- exit
- We repeated this for all interfaces with different IP ranges (e.g., 192.168.2.1 for Fa0/1).
- 5. Enabled RIP Protocol:
 - In global configuration mode, we typed:
 - router rip
 - version 2 to ensure classless routing.
- 6. Added Networks to RIP:
 - We mentioned the networks directly connected to the router:
 - network 192.168.1.0
 - network 192.168.2.0
- 7. Saved the Configuration:
 - We typed exit to leave RIP configuration mode and saved the changes by entering:
 - wr or copy running-config startup-config.

The setup was completed, and the routers successfully shared routing information using RIP, allowing smooth communication across networks.

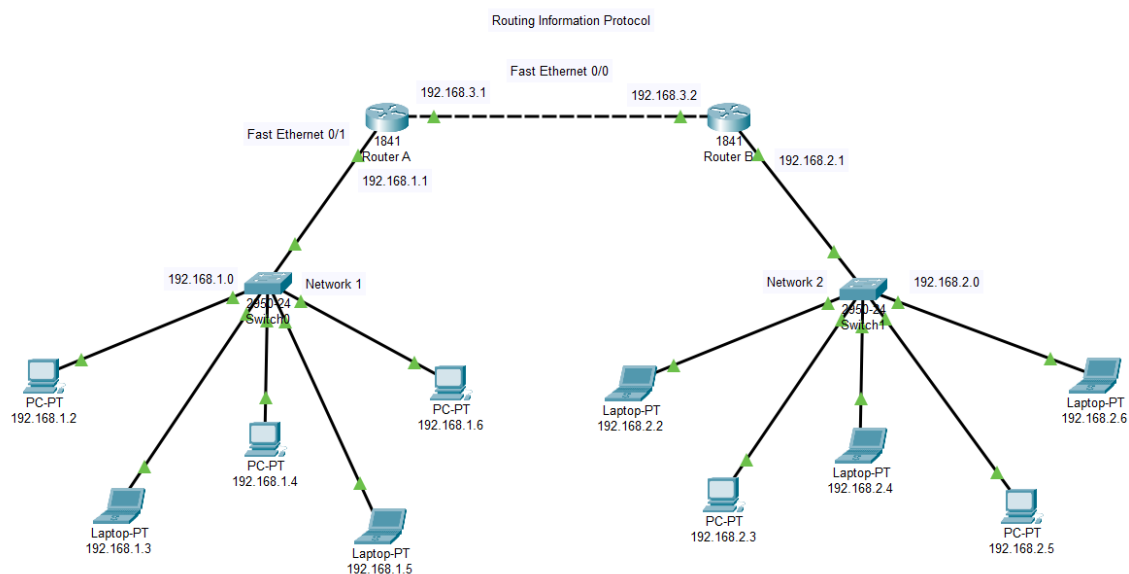


Figure 01: Configuration of Routing Information Protocol (RIP).

CLI Command of Router A:

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int fa0/1

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#int fa0/0

Router(config-if)#ip address 192.168.3.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

Router(config)#exit

Router#

%SYS-5-CONFIG_I: Configured from console by console

Router#wr

Building configuration...

[OK]

Router#
```

CLI Command of Router B:

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int fa0/0

Router(config-if)#ip address 192.168.3.2 255.255.255.0

Router(config-if)#no shut

Router(config-if)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#int fa0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
```

RIP Configuration of Router A:

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router RIP
Router(config-router)#version 2
Router(config-router)#net 192.168.1.0
Router(config-router)#net 192.168.3.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
```

RIP Configuration of Router B:

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router RIP
Router(config-router)#version 2
```

```

Router(config-router)#net 192.168.3.0
Router(config-router)#net 192.168.2.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]

```

Simulation Process:

- **Method 1: Router CLI Command:**

We used the router's CLI to assign IP addresses, enable RIP, and configure network settings for proper communication.

```

Router#
Router#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

R 192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:23, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/1
C 192.168.3.0/24 is directly connected, FastEthernet0/0

```

- **Method 2: Sending Packets**

We sent packets between devices to test if data could travel across the networks, confirming successful routing.









| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num |
|---|-------------|-------------|-------------|------|---|-----------|----------|-----|
|  | Successful | 192.168.1.2 | 192.168.2.4 | ICMP |  | 0.000 | N | 0 |
|  | Successful | 192.168.2.5 | 192.168.1.4 | ICMP |  | 0.000 | N | 1 |
|  | Successful | 192.168.1.6 | 192.168.2.2 | ICMP |  | 0.000 | N | 2 |
|  | Successful | 192.168.2.5 | 192.168.1.3 | ICMP |  | 0.000 | N | 3 |

Figure 02: Simulation process using the packet symbol.

- **Method 3: Ping Test**

We performed a ping test to check connectivity between devices by sending ICMP packets, ensuring communication was smooth without packet loss.

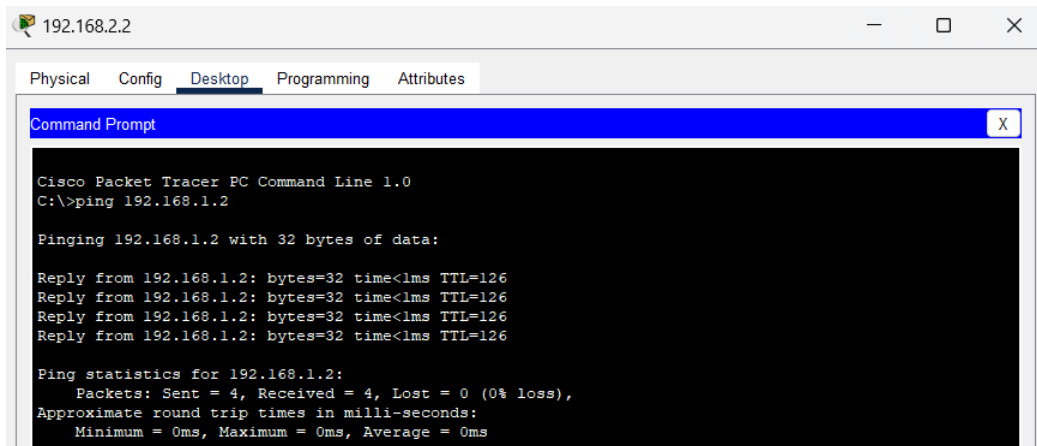


Figure 03: Simulation process using the ping test.

Results and Discussion: The RIP (Routing Information Protocol) configuration was successfully applied. After assigning IP addresses and enabling RIP on the router interfaces, the routers exchanged routing information, allowing data packets to be routed between different networks. The correct RIP version ensured compatibility, and all devices communicated without issues, verifying that the network was properly configured.

Precautions:

1. Ensure that **each interface** has the correct IP address and subnet mask.
2. Use **RIP version 2** to avoid classful routing issues.
3. Verify that **cables are correctly connected** between routers, switches, and PCs.
4. Save the configuration to avoid losing changes after a reboot.
5. Ensure all routers are within the same **RIP domain** for proper route sharing.

Experiment Number: 06

Name of the Experiment: Configure Open Shortest Path First (OSPF) Routing Protocol.

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Switch.
 2. UTP Cable (Straight Through).
 3. End Devices (Desktop, Laptop).
 4. IP Address (192.168.1.x, 192.168.2.x & 192.168.3.x)
 5. Router.
 6. Copper crossover cable.

Description: Open Shortest Path First (OSPF) is a link-state routing protocol used in Internet Protocol (IP) networks. It enables routers to dynamically share routing information, allowing them to determine the most efficient paths for data transmission. OSPF operates within a single autonomous system and is designed to be scalable and efficient, making it suitable for larger networks. It uses a hierarchical structure, dividing networks into areas to optimize routing and reduce overhead. OSPF calculates the shortest path using Dijkstra's algorithm and supports features like fast convergence, authentication, and load balancing.

Configuration Process (Completed):

1. Placed Devices:
 - We dragged and dropped two routers, two switches, and multiple PCs/laptops onto the workspace.
2. Connected Devices:
 - We used straight-through cables to connect:
 - PCs/laptops to their respective switches.
 - Each switch to a router.
 - The two routers through their Fast Ethernet ports.
3. Configured Routers:
 - On each router, we assigned IP addresses to the connected interfaces.
 - We enabled OSPF routing and assigned the relevant networks to OSPF areas.
4. Assigned IPs to End Devices:
 - We set the IP addresses for the PCs and laptops:
 - Devices in Network 1 were given IPs in the range 192.168.1.x.
 - Devices in Network 2 were assigned IPs in the range 192.168.2.x.

- The appropriate default gateway was configured on all devices.

5. Tested Connectivity:

- Finally, we performed ping tests between devices on different networks. The successful pings confirmed that OSPF routing was working correctly and the setup was complete.

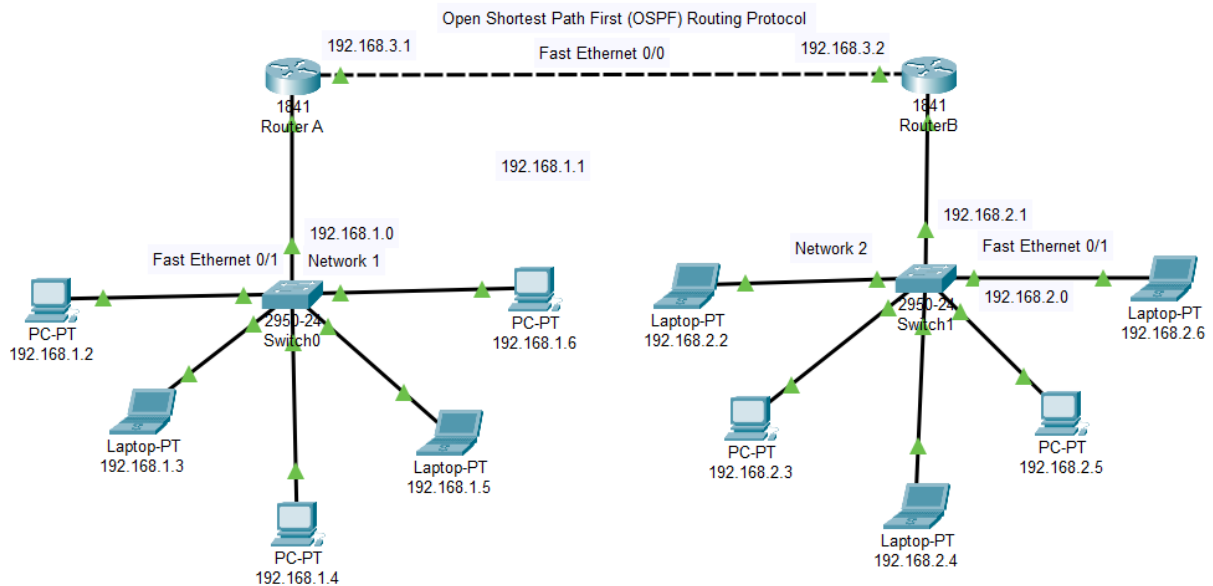


Figure 01: Configuration of Open Shortest Path First (OSPF) Routing Protocol.

CLI Command of Router A:

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int fa0/0

Router(config-if)#ip address 192.168.3.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#int fa0/1

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up


```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
```

CLI Command of Router B:

--- System Configuration Dialog ---

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#int fa0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
Router#
```

OSPF Configuration of Router A:

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
Router#wr
Building configuration...
[OK]
```

OSPF Configuration of Router B

```
Router#enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
```

Simulation Process:

- **Method 1: Router CLI Command:**

We used the router's CLI to assign IP addresses, enable RIP, and configure network settings for proper communication.

```
Router#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route
 Gateway of last resort is not set
 C 192.168.1.0/24 is directly connected, FastEthernet0/1
 O 192.168.2.0/24 [110/2] via 192.168.3.2, 00:03:12, FastEthernet0/0
 C 192.168.3.0/24 is directly connected, FastEthernet0/0

• Method 2: Ping Test

We performed a ping test to check connectivity between devices by sending ICMP packets, ensuring communication was smooth without packet loss.

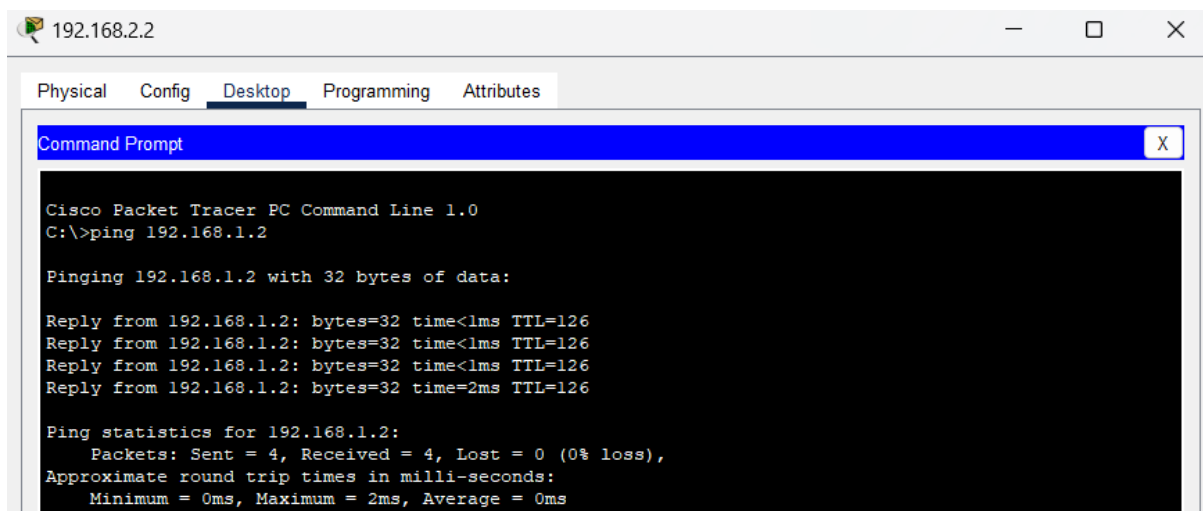


Figure 02: Simulation process using the ping test.

• Method 3: Sending Packets

We sent packets between devices to test if data could travel across the networks, confirming successful routing.

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|------|-------------|-------------|-------------|------|-------|-----------|----------|-----|--------|
| | Successful | 192.168.1.6 | 192.168.2.6 | ICMP | | 0.000 | N | 3 | (edit) |
| | Successful | 192.168.2.6 | 192.168.1.6 | ICMP | | 0.000 | N | 4 | (edit) |
| | Successful | 192.168.1.3 | 192.168.2.2 | ICMP | | 0.000 | N | 5 | (edit) |
| | Successful | 192.168.2.5 | 192.168.1.5 | ICMP | | 0.000 | N | 6 | (edit) |

Figure 03: Simulation process using the packet symbol.

Results and Discussion: The OSPF (Open Shortest Path First) configuration was successfully implemented. After assigning IP addresses and enabling OSPF on the router interfaces, the routers began exchanging link-state information, which allowed for efficient routing of data packets across different networks. The use of OSPF's area configuration optimized the routing process and ensured scalability for future expansion. All devices communicated effectively, confirming that the network was correctly set up and that OSPF was functioning as intended.

Precautions:

1. Ensure that each interface is assigned the correct IP address and subnet mask.
2. Define OSPF areas appropriately to enhance network performance and manageability.
3. Verify that all cables are properly connected between routers, switches, and end devices.
4. Save the configuration changes to prevent loss after a reboot.
5. Ensure all routers are configured with matching OSPF process IDs and are in the same OSPF area to facilitate proper route sharing.

Experiment Number: 07

Name of the Experiment: Configure Enhanced Interior Gateway Routing Protocol (EIGRP).

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Switch.
 2. UTP Cable (Straight Through).
 3. End Devices (Desktop, Laptop).
 4. IP Address (192.168.1.x, 192.168.2.x & 192.168.3.x)
 5. Router.
 6. Serial DCE cable.

Description: Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol developed by Cisco for efficient data routing within an autonomous system. It combines features of both distance-vector and link-state protocols, offering fast convergence, scalability, and loop-free routing. EIGRP uses metrics like bandwidth, delay, load, and reliability to determine the best path. It supports VLSM (Variable Length Subnet Mask) and unequal-cost load balancing, making it more flexible than traditional protocols. EIGRP routers exchange partial updates only when changes occur, minimizing network overhead.

Configuration Process (Completed):

1. Placed Devices:
 - We deployed two routers, two switches, and multiple PCs/laptops onto the workspace.
2. Connected Devices:
 - Straight-through cables were used to establish connections:
 - PCs and laptops were connected to their respective switches.
 - Each switch was connected to a router.
 - The two routers were linked via their Fast Ethernet ports.
3. Configured Routers:
 - We assigned IP addresses to the routers' interfaces connected to their respective networks.
 - EIGRP routing was enabled, and the connected networks were added to the EIGRP configuration for dynamic route sharing.
4. Assigned IPs to End Devices:
 - We configured IP addresses for the PCs and laptops as follows:

- Devices in Network 1 were assigned IPs within the 192.168.1.x range.
- Devices in Network 2 received IPs in the 192.168.2.x range.
- The correct default gateway (the router interface IP) was set on each device to ensure proper routing.

5. Tested Connectivity:

- To verify the setup, we conducted ping tests between devices in different networks. All tests were successful, confirming that EIGRP was functioning properly and the network was configured correctly.

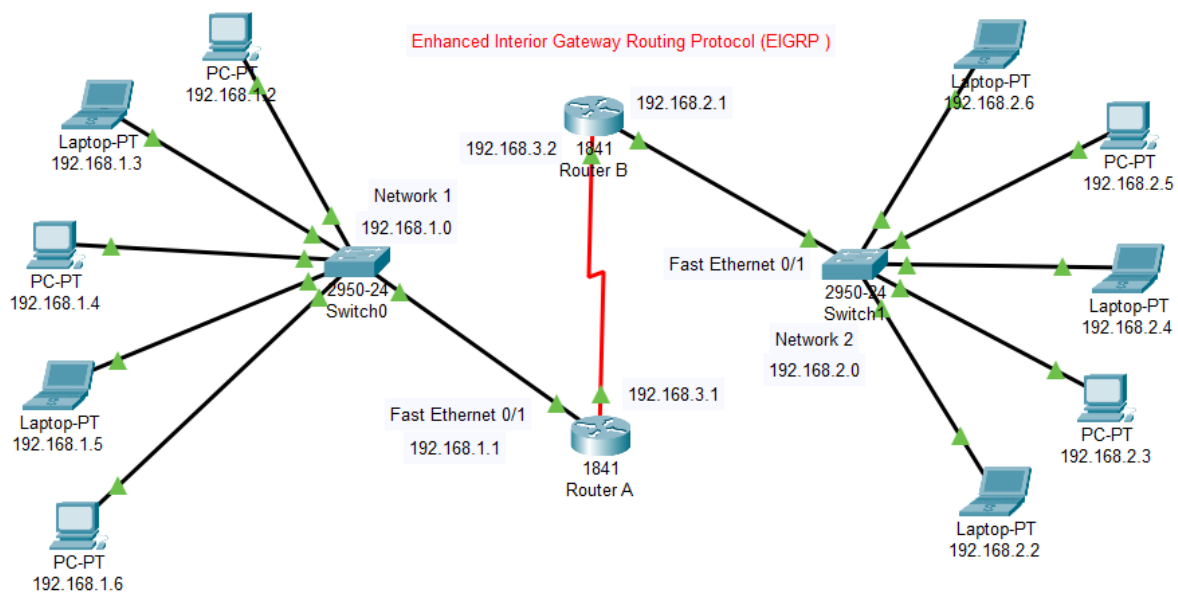


Figure 01: Configuration of Enhanced Interior Gateway Routing Protocol (EIGRP).

CLI Command of Router B:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#int serial0/0/0
```

```
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#exit
```

EIGRP Configuration of Router B

```
Router#config t
Router(config)#router eigrp 10
Router(config-router)#network 192.168.3.0 255.255.255.0
Router(config-router)#network 192.168.2.0 255.255.255.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#copy running-config startup-config
Destination filename [startup-config]?
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.3.1 (Serial0/0/0) is up: new adjacency
Building configuration...
[OK]
```

CLI Command of Router A:

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#int serial0/0/0
Router(config-if)#ip address 192.168.3.1
```

```
% Incomplete command.
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

EIGRP Configuration of Router A

```
Router(config)#router eigrp 10
Router(config-router)#network 192.168.1.0 255.255.255.0
Router(config-router)#network 192.168.3.0 255.255.255.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.3.2 (Serial0/0/0) is up: new adjacency
Router(config-router)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#copy runn
% Incomplete command.
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Simulation Process:

- **Method 1: Router CLI Command:**

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
C 192.168.1.0/24 is directly connected, FastEthernet0/1
D 192.168.2.0/24 [90/20514560] via 192.168.3.2, 00:08:41, Serial0/0/0
C 192.168.3.0/24 is directly connected, Serial0/0/0
```


- **Method 2: Ping Test**

We performed a ping test to check connectivity between devices by sending ICMP packets, ensuring communication was smooth without packet loss.

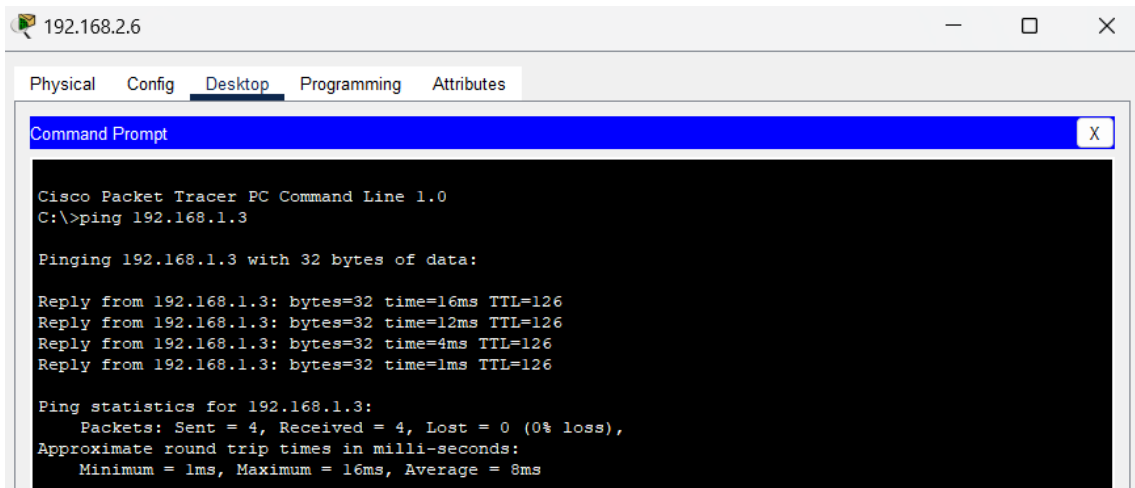


Figure 02: Simulation process using the ping test.

- **Method 3: Sending Packets**

We sent packets between devices to test if data could travel across the networks, confirming successful routing.







| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|---|-------------|-------------|-------------|------|---|-----------|----------|-----|--------|
|  | Successful | 192.168.2.3 | 192.168.1.6 | ICMP |  | 0.000 | N | 0 | (edit) |
|  | Successful | 192.168.1.2 | 192.168.2.4 | ICMP |  | 0.000 | N | 1 | (edit) |
|  | Successful | 192.168.2.6 | 192.168.1.4 | ICMP |  | 0.000 | N | 2 | (edit) |

Figure 03: Simulation process using the packet symbol.

Results and Discussion: The EIGRP configuration was successfully implemented. After assigning IP addresses and enabling EIGRP on the routers, they exchanged routing information, allowing seamless communication between devices in different networks. Ping tests between devices confirmed that the setup was correct and EIGRP was functioning as expected.

Precautions:

1. Ensure correct IP addressing and subnet masks on all devices.
2. Use matching EIGRP process IDs across routers.
3. Verify proper cabling between routers, switches, and PCs.
4. Confirm all routers belong to the same autonomous system for route sharing.

Experiment Number: 08

Name of the Experiment: Configure Virtual Local Area Network (VLAN).

Experimental Requirement:

- **Required Software:** Cisco Packet Tracer for Simulation.
- **Required Components:**
 1. Switch.
 2. UTP Cable (Straight Through).
 3. End Devices (Desktop, Laptop).
 4. IP Address (192.168.1.x)
 5. Copper crossover cable.

Description: A VLAN (Virtual Local Area Network) is a logical grouping of devices within a network that allows them to communicate as if they were on the same physical LAN, even if they are physically located on different network segments. VLANs are primarily used to create isolated network segments within a larger network, which enhances security, manages traffic flow, and improves network efficiency. By segmenting the network, VLANs help reduce broadcast traffic, minimize congestion, and control which devices can communicate with each other.

In this setup, VLANs were used to create two distinct groups: *Faculty and Students*. Devices assigned to the Faculty VLAN can communicate exclusively with other faculty devices, while Student VLAN devices are similarly restricted to communication within their own group. This separation provides security, ensuring that students cannot access faculty resources and vice versa. Additionally, VLANs make it easier to manage and control network resources, as each group can have tailored network policies and configurations suited to their specific needs. This logical segmentation not only isolates network traffic but also reduces broadcast domains, improving overall performance.

Configuration Process (Completed):

1. Placed Components:
 - We added two switches (Switch A and Switch B) and multiple end devices (PCs and Laptops) for the Faculty and Students networks in Cisco Packet Tracer.
2. Created VLANs on Each Switch:
 - On Switch A, we created two VLANs: one for the Faculty network and another for the Students network, naming them accordingly.
 - We repeated this process on Switch B to ensure consistency across both switches.
3. Assigned Ports to VLANs on Switch A:
 - We assigned specific ports on Switch A to the Faculty VLAN for devices located in the Faculty section of the network.

- Similarly, we assigned other ports to the Students VLAN for the devices located in the students section.
4. Assigned Ports to VLANs on Switch B:
 - On Switch B, we mirrored the VLAN assignments by assigning corresponding ports to the Faculty VLAN and Students VLAN, matching the configuration on Switch A.
 5. Configured the Trunk Port Between Switches:
 - To allow communication between the two switches for both VLANs, we configured a trunk link on the ports connecting Switch A and Switch B. This allowed VLAN traffic to pass through the link and ensured proper connectivity between both switches.
 6. Assigned IP Addresses to End Devices:
 - We assigned IP addresses to each Faculty device within a specified range that corresponded to the Faculty VLAN.
 - Similarly, we assigned IP addresses to Student devices in a range that matched the Students VLAN.
 7. Tested Connectivity:
 - After completing the configuration, we tested the setup by verifying that devices within the same VLAN could communicate with each other.
 - We also checked that devices from different VLANs were isolated, confirming that they couldn't communicate across VLAN boundaries.

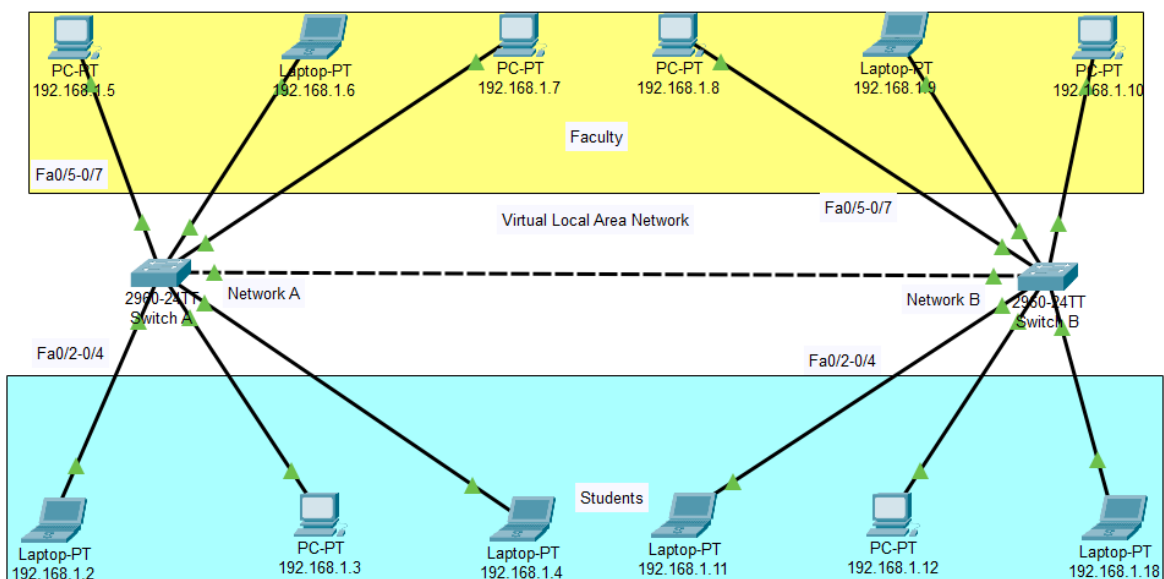


Figure 1: VLAN and trunk configuration.

CLI Command for both Router A and B:

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Faculty
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Students
Switch(config-vlan)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fa0/4
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fa0/5
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int fa0/6
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int fa0/7
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#exit
```

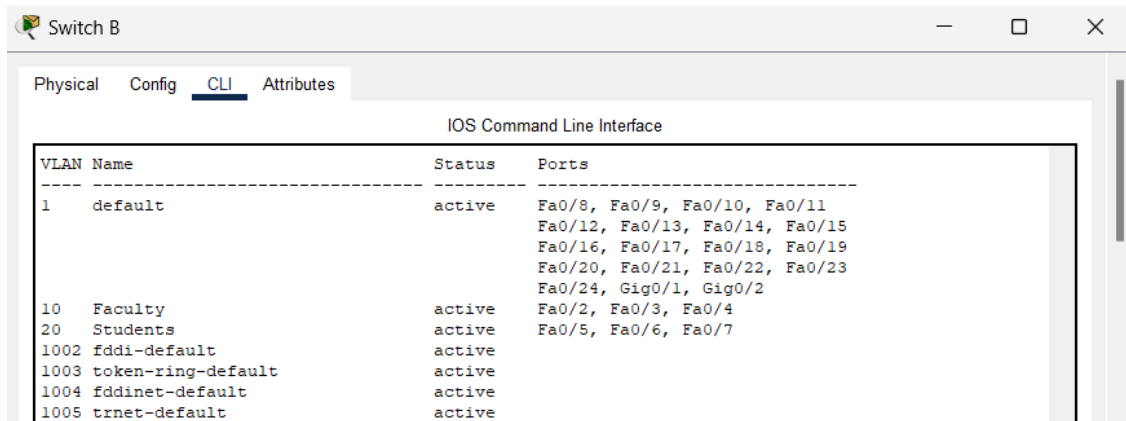
Trunk Configuration for both Router A and B

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config)#int range fa0/2-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#exit
```

Simulation Process:

- **Method 1: Switch CLI Command**

This configuration shows two active VLANs: **VLAN 10 (Faculty)** and **VLAN 20 (Students)**. Ports `Fa0/2` to `Fa0/4` are assigned to Faculty, while ports `Fa0/5` to `Fa0/7` are designated for Students. The **default VLAN (VLAN 1)** includes all other unassigned ports. This setup ensures isolated communication within each VLAN, simulating network segmentation between Faculty and Students.



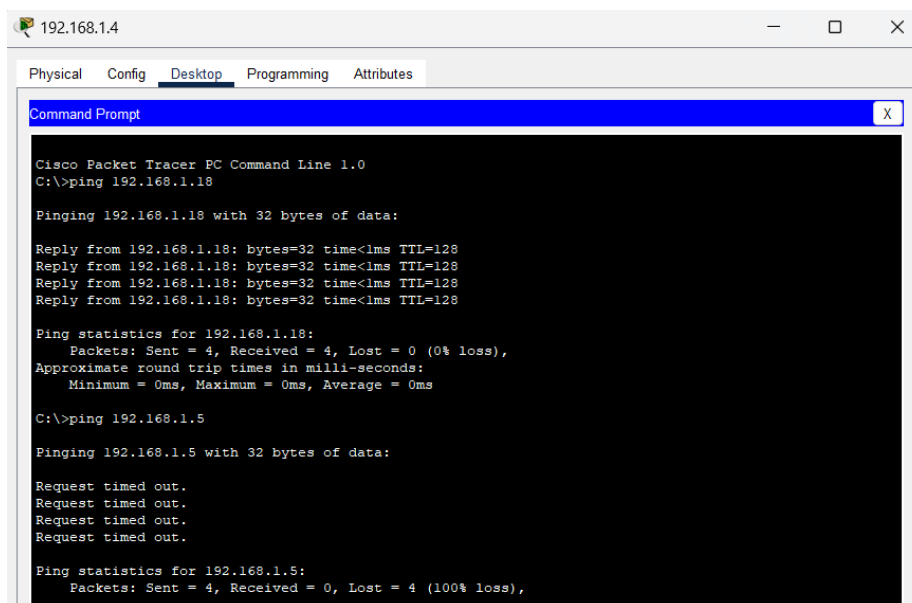
The screenshot shows the CLI of Switch B with the following VLAN configuration:

| VLAN | Name | Status | Ports |
|------|--------------------|--------|--|
| 1 | default | active | Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2 |
| 10 | Faculty | active | Fa0/2, Fa0/3, Fa0/4 |
| 20 | Students | active | Fa0/5, Fa0/6, Fa0/7 |
| 1002 | fddi-default | active | |
| 1003 | token-ring-default | active | |
| 1004 | fdnet-default | active | |
| 1005 | trnet-default | active | |

Figure 02: Simulation process the CLI Command.

- **Method 2: Ping Test**

A ping test was conducted to evaluate connectivity between devices within the same VLAN by sending ICMP packets. This test confirmed that devices within the same VLAN were able to communicate effectively, as indicated by successful replies. However, devices in different VLANs did not receive replies, highlighting the isolation of traffic between VLANs.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.18

Pinging 192.168.1.18 with 32 bytes of data:

Reply from 192.168.1.18: bytes=32 time<1ms TTL=128
Reply from 192.168.1.18: bytes=32 time<1ms TTL=128
Reply from 192.168.1.18: bytes=32 time<1ms TTL=128
Reply from 192.168.1.18: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 03: Simulation process using the ping test.

- **Method 3: Sending Packets**

Packets were transmitted between devices to assess data transmission across the same VLAN, verifying that successful routing occurred within the VLAN. In contrast, attempts to send packets between different VLANs did not yield responses, demonstrating the segregation of network traffic and the routing constraints between VLANs.









| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num |
|---|-------------|--------------|--------------|------|--|-----------|----------|-----|
|  | Successful | 192.168.1.2 | 192.168.1.11 | ICMP |  | 0.000 | N | 0 |
|  | Failed | 192.168.1.5 | 192.168.1.4 | ICMP |  | 0.000 | N | 1 |
|  | Failed | 192.168.1.18 | 192.168.1.6 | ICMP |  | 0.000 | N | 2 |
|  | Successful | 192.168.1.5 | 192.168.1.10 | ICMP |  | 0.000 | N | 3 |

Figure 04: Simulation process by sending packets.

Results and Discussion

i. Ping Test Results

- **Same VLAN:** Successful pings confirmed effective communication among devices, with no packet loss.
- **Different VLANs:** Pings to devices in other VLANs resulted in timeouts, indicating isolation between VLANs.

ii. Packet Sending Results

- **Same VLAN:** Packets were successfully transmitted and acknowledged, confirming proper routing.
- **Different VLANs:** Attempts to send packets to devices in other VLANs failed, reinforcing the need for routing to facilitate inter-VLAN communication.

Precautions

Accurate Setup: Mirror real network settings in the simulation.

Resource Allocation: Ensure adequate CPU and RAM for performance.

Monitoring: Use tools to track network behavior in real-time.

Parameter Validation: Confirm simulation parameters match real-world conditions.

Backup Configurations: Regularly save simulation setups to prevent data loss.