Tuhin 252-56-012 Cyber security Lab

Tanjim Tuhin

January 2025

1 Introduction

The **Open Systems Interconnection (OSI) Model** is a conceptual framework that standardizes network communication into seven layers. Each layer serves a specific role, ensuring seamless data transmission between devices.

2 Layers of the OSI Model(Day 2)

2.1 Physical Layer

The **Physical Layer** is responsible for transmitting raw binary data over a physical medium, such as cables, fiber optics, or radio waves. It deals with signals, voltages, and data rates.

2.2 Data Link Layer

This layer ensures reliable data transfer between directly connected devices. It uses **MAC (Media Access Control)** and **LLC (Logical Link Control)** for addressing and error detection.

2.3 Network Layer

The **Network Layer** is responsible for routing data across multiple networks using logical addressing (e.g., IP addresses). It determines the optimal path for data transmission.

2.4 Transport Layer

This layer ensures reliable communication through error correction and flow control. Protocols like **TCP (Transmission Control Protocol)** and **UDP (User Datagram Protocol)** operate at this level.

2.5 Session Layer

The **Session Layer** establishes, maintains, and terminates connections between applications. It enables dialogue control between devices.

2.6 Presentation Layer

This layer ensures proper data formatting, encryption, and compression for compatibility between systems.

2.7 Application Layer

The **Application Layer** interacts directly with users through software applications like web browsers, email clients, and file transfer services.

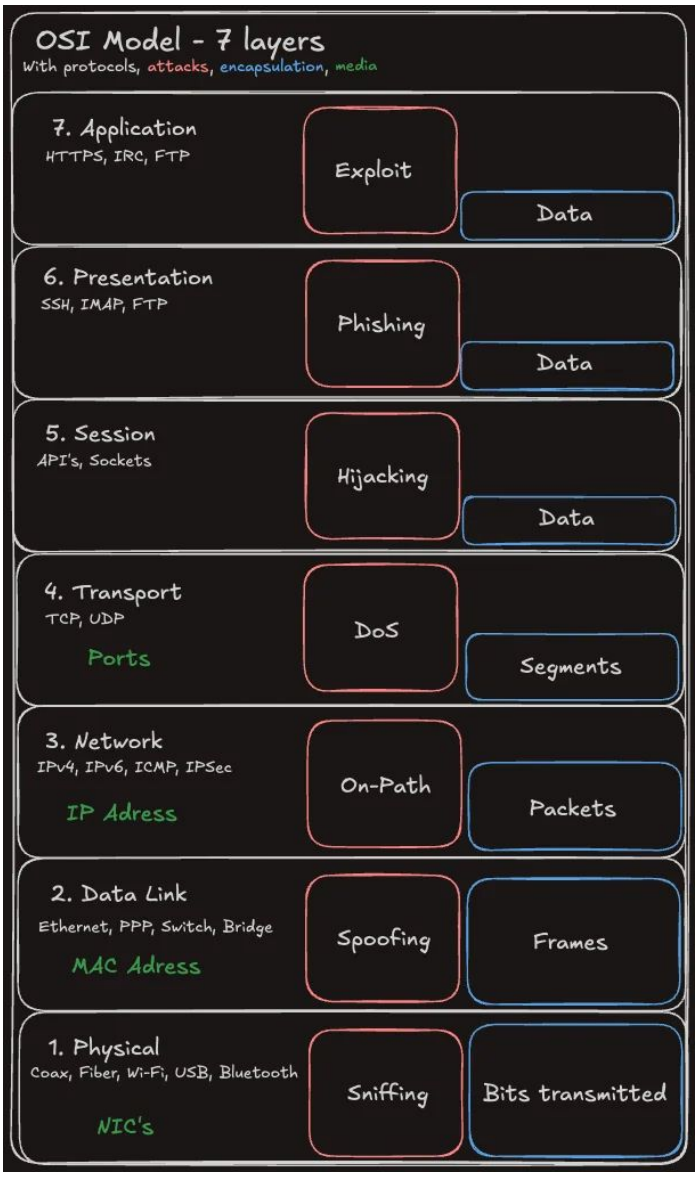

Figure 1: OSI model with potential attack

The OSI model has 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. It standardizes how data is transmitted over networks, from raw bits to user applications. Each layer serves a specific function like routing, encryption, or error handling.

3 Cisco Packet Tracer(Day 3)

Ethernet Cables:
Ethernet connectivity forms the backbone of modern networking infrastructure, providing reliable data transmission between computers, routers, switches, and other networking devices. The type of Ethernet cable used significantly impacts network functionality and efficiency. Two commonly used cables are straight-through cables and crossover cables, each designed for specific applications based on their wiring configurations.

Straight vs Crossover Cable:
A ***straight-through cable***, also known as a standard Ethernet cable, has the same wiring configuration on both ends. This means that the order of wires remains consistent from one connector to the other.

Uses of a Straight-Through Cable. [Connecting different types of devices] such as:

- PC to Switch
- Router to Switch
- Modem to Router

A **crossover cable** is a special type of Ethernet cable where the transmit (Tx) and receive (Rx) wires are swapped on one end. This means that one end follows the T568A standard, while the other follows the T568B standard.

Uses of a Crossover Cable. [Directly connecting similar devices]
such as:

- PC to PC
- Switch to Switch
- Router to Router

3.1 Connecting Two End Device

making a network topology connecting two same types of end devices needs special types of ethernet cable like crossover cable without needing switch or router. It swaps the transmit (Tx) and receive (Rx) wires, allowing devices to communicate properly. This setup is commonly used for peer-to-peer networking, file sharing, or testing network configurations in a small-scale environment. For this type of topology need an ethernet cable, but now in modern devices often support Auto-MDI/X, meaning they can automatically detect the cable type, allowing a standard Ethernet cable to work instead of a crossover cable.

HUB vs Switch vs Router

Hub: The Basic Connector A hub is the simplest networking device that operates at the Physical Layer (Layer 1) of the OSI model. It acts as a repeater, broadcasting data to all connected devices, regardless of the destination.

Key Features: Sends data to all devices, causing network congestion. Works on a single collision domain, leading to more data collisions. Cannot differentiate between devices or manage traffic.

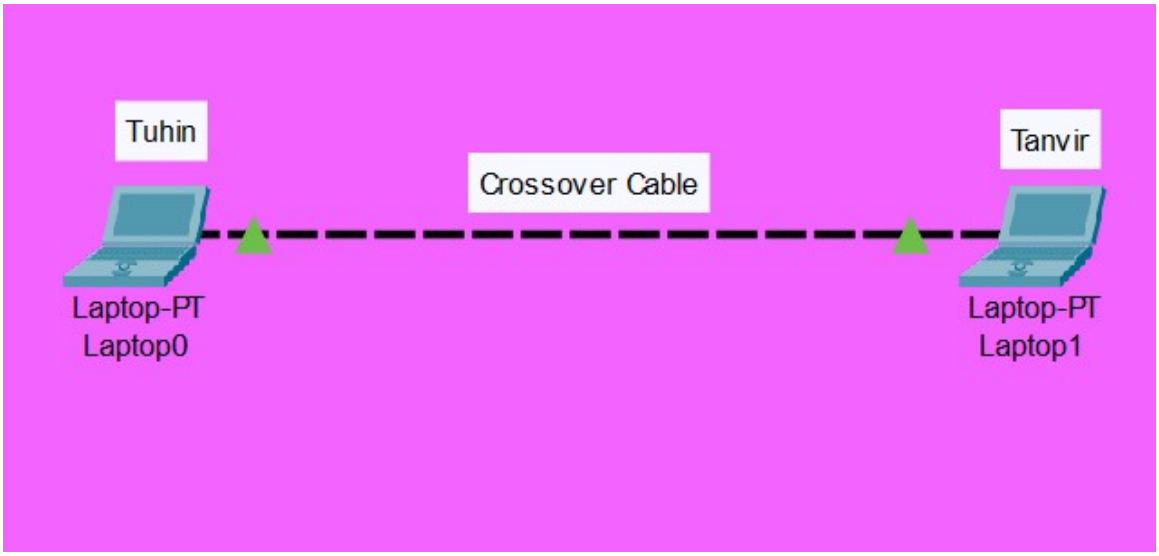

Figure 2: Connecting Two End Device

Mostly outdated and replaced by switches.

Switch: The Smart Distributor A switch operates at the Data Link Layer (Layer 2) and is more intelligent than a hub. It uses MAC addresses to forward data only to the intended recipient, improving network efficiency.

Key Features: Sends data only to the intended device, reducing congestion. Each port has its own collision domain, preventing collisions. Can support VLANs for better traffic management. Widely used in modern LANs for better performance.

Router: The Network Manager A router is the gateway of a network. It operates at the Network Layer (Layer 3) and is responsible for directing data between different networks. It uses IP addresses to determine the best path for data transmission.

Key Features: Connects different networks, including LANs and the internet. Uses IP addresses for efficient data routing. Can provide firewall security features. Creates multiple broadcast domains, improving network segmentation.

Conclusion:
A hub is outdated and simply forwards data to all devices.
A switch improves network efficiency by directing data only to the intended device.
Hubs and Switches are used to exchange data within a local area network
A router connects networks by reading IP address and enables internet communication.

3.2 Developing a network using HUB

A hub-based network is a simple way to connect multiple devices in a LAN, though it lacks efficiency compared to switches. In Cisco Packet Tracer, creating such a network involves placing a hub and connecting multiple PCs using straight-through Ethernet cables. Once connected, assign IP addresses manually or enable DHCP if a router is included. Since hubs operate at Layer 1 (Physical Layer) of the OSI model, they broadcast data to all devices, leading to collision domains and network congestion. To test connectivity, use the ping command in the command prompt of each PC. While

hubs are outdated due to their inefficiency and lack of security, this setup helps understand basic networking concepts. The diagram in Packet Tracer will illustrate device connections, demonstrating how data flows in a hub-based network. However, for better performance, replacing the hub with a switch is recommended to reduce collisions and improve speed.

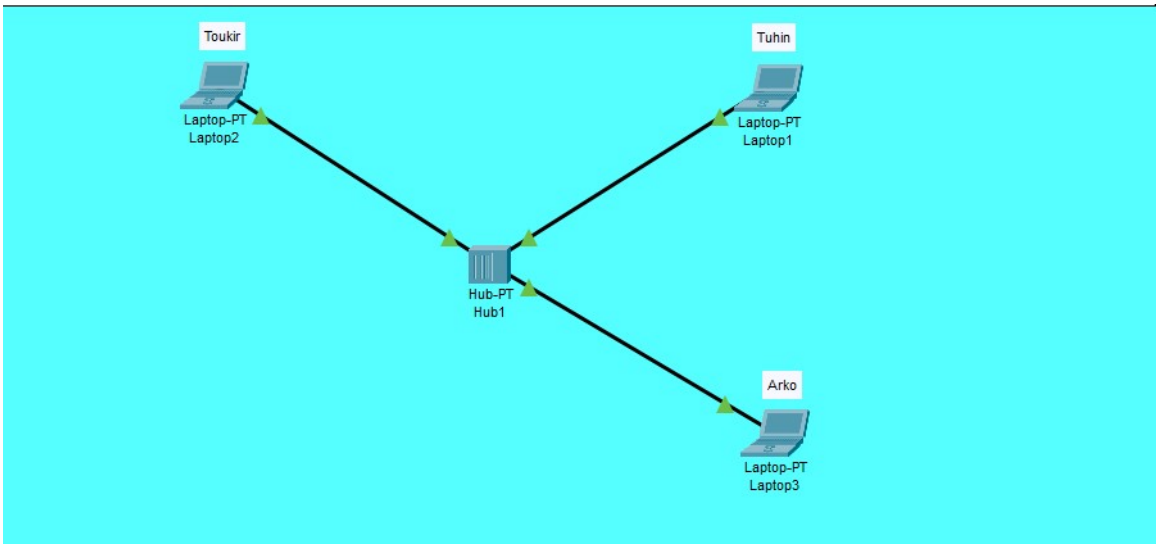

Figure 3: Developing a network using HUB

3.3 Developing a network using Switch

article graphicx

Developing Two Networks Using Switches in Cisco Packet Tracer

A **switch-based network** enhances performance by forwarding data only to the intended recipient, reducing congestion. To create two separate networks using switches in Cisco Packet Tracer, place two switches and connect multiple PCs using straight-through Ethernet cables. Assign different IP subnets for each network (e.g., **192.168.1.0/24** and **192.168.2.0/24**). Since switches operate at Layer 2 (Data Link Layer) of the OSI model, they rely on MAC addresses for efficient data transfer. However, devices in different subnets cannot communicate directly. To enable internetwork communication, add a router or configure a Layer 3 switch with VLANs and inter-VLAN routing. In Packet Tracer, test connectivity using the `ping` command between devices in the same and different networks. This setup demonstrates segmentation, traffic isolation, and efficient data forwarding, making it suitable for enterprise environments where multiple networks need controlled communication. The diagram will show two networks connected via a router or Layer 3 switch for interconnectivity.

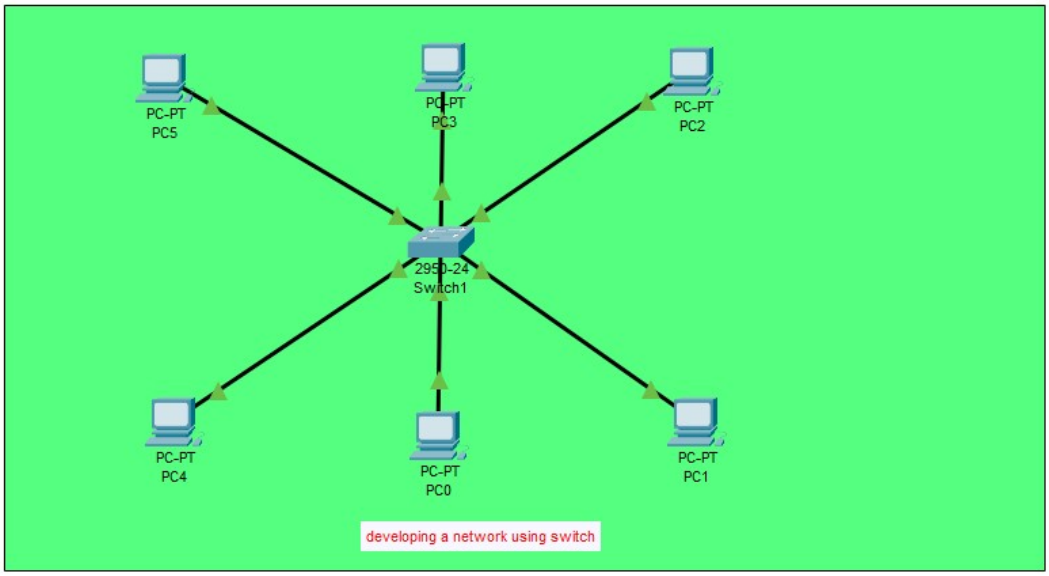

Figure 4: Developing a network using Switch

3.4 Developing two networks using Switches

A switch-based network enhances performance by forwarding data only to the intended recipient, reducing congestion. To create two separate networks using switches in Cisco Packet Tracer, place two switches and connect multiple PCs using straight-through Ethernet cables. Assign different IP subnets for each network (e.g., `192.168.1.0/24` and `192.168.2.0/24`). Since switches operate at Layer 2 (Data Link Layer) of the OSI model, they rely on MAC addresses for efficient data transfer. However, devices in different subnets cannot communicate directly. To enable inter-network communication, add a router or configure a Layer 3 switch with VLANs and inter-VLAN routing. In Packet Tracer, test connectivity using the `ping` command between devices in the same and different networks. This setup demonstrates segmentation, traffic isolation, and efficient data forwarding, making it suitable for enterprise environments where multiple networks need controlled communication. The diagram will show two networks connected via a router or Layer 3 switch for interconnectivity.

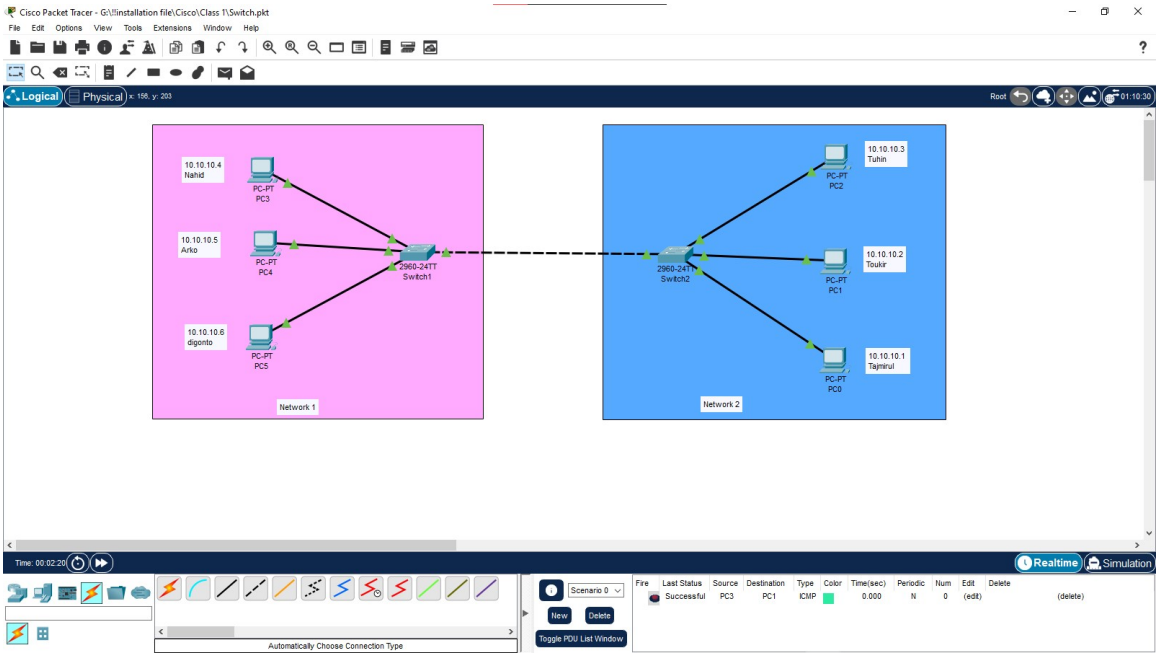

Figure 5: Developing two networks using Switches

4 Cisco Packet Tracer(Day 04)

Router A router is a networking device that connects multiple networks and directs data packets between them. It operates at Layer 3 (Network Layer) of the OSI model, using IP addresses to determine the best path for data transmission. Unlike switches, which forward data based on MAC addresses within the same network, routers enable communication between different subnets by analyzing and forwarding packets to their destination. Routers can be configured with static routes or use dynamic routing protocols like RIP, OSPF, and BGP to adapt to network changes. They also provide security features such as firewall capabilities, NAT (Network Address Translation), and VPN support, making them essential for both home and enterprise networks. In Cisco Packet Tracer, routers facilitate inter-network communication by connecting different subnets, allowing devices in separate networks to communicate efficiently. By testing connectivity with commands like `ping` and `traceroute`, users can verify routing configurations and troubleshoot network issues.

Our picture shows a basic network topology using a router and two end devices (laptops) connected in separate subnets. The router has two interfaces:

- 192.168.1.1 (connected to Laptop0)
- 192.168.2.1 (connected to Laptop1)

Each laptop is assigned an IP address within its respective subnet:

- Laptop0 has 192.168.1.2
- Laptop1 has 192.168.2.2

The router serves as the intermediary, enabling communication between the two different subnets.

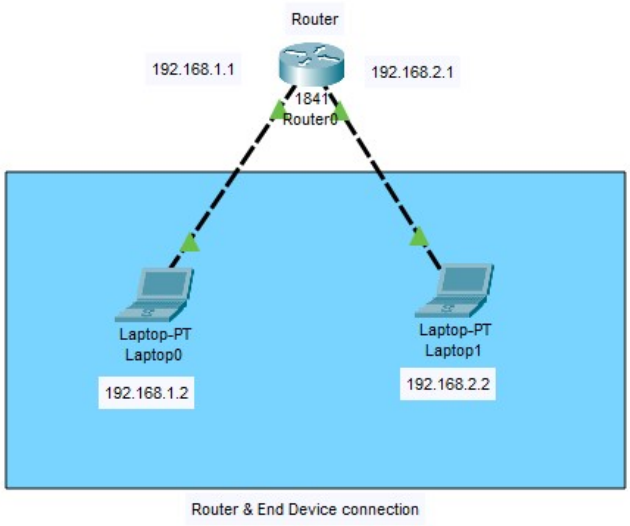

Figure 6: Router End devices connection

4.1 Router connection with two LAN

A router can connect two separate Local Area Networks (LANs), enabling communication between devices in different network segments. Each LAN is typically on a different IP subnet. The router has an interface connected to each LAN, with its own IP address within that LAN's subnet, acting as the gateway for devices within that LAN. By maintaining routing tables, the router determines the best path to forward data packets between the two LANs, effectively bridging the network segments and allowing resource sharing and inter-network communication.

4.1.1 Router connection using CLI command

The network topology consists of a router connecting two local area networks (LANs) via two switches (Switch-1 and Switch-2). LAN-1 includes three PCs (PC-PT0, PC-PT1, PC-PT2) with IP addresses in the 10.10.10.0/24 subnet. LAN-2 includes three laptops (Laptop-PT1, Laptop-PT2, Laptop-PT3) with IP addresses in the 192.168.1.0/24 subnet. The router interfaces are configured as follows:

- GigabitEthernet0/0 connects to Switch-1 (LAN-1) with IP 10.10.10.100/24.
- GigabitEthernet0/1 connects to Switch-2 (LAN-2) with IP 192.168.1.100/24.

The CLI (Command Line Interface) commands are used to configure the router to enable communication between these two LANs.

Explanation of CLI Commands The CLI commands provided are executed on the router to configure its interfaces. Below is a step-by-step breakdown of the commands and their purpose:

- **Enter Privileged EXEC Mode** (`enable`): This command grants administrative access to the router, allowing configuration changes.

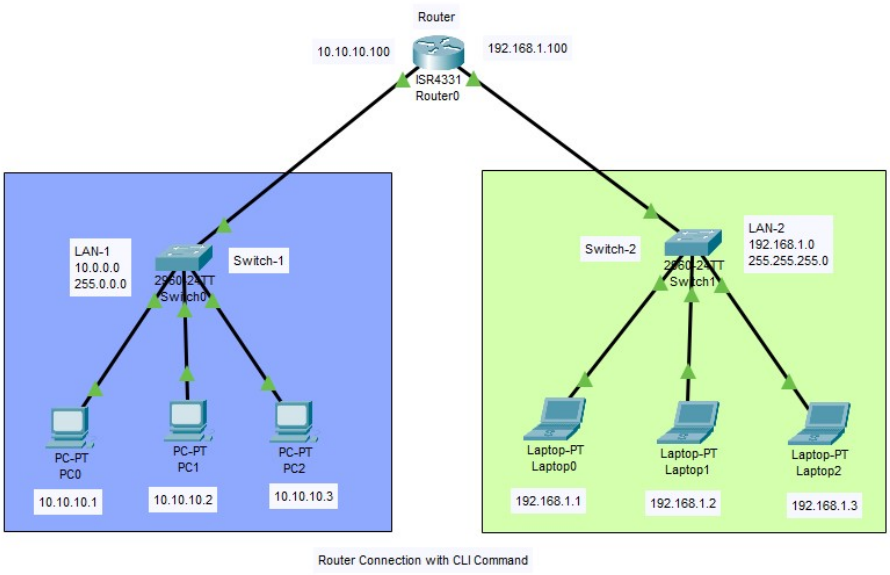

Figure 7: Router connection using CLI command

- **Enter Global Configuration Mode** (`Configure terminal`): This mode allows modification of the router's global settings, such as interface configurations.
- **Select Interface for Configuration** (`interface GigabitEthernet0/0`): Specifies the first interface (GigabitEthernet0/0) connected to Switch-1 (LAN-1) for configuration.
- **Assign IP Address and Subnet Mask** (`ip address 10.10.10.100 255.255.255.0`): Assigns the IP address 10.10.10.100 with a subnet mask of 255.255.255.0 (indicating a /24 subnet) to the GigabitEthernet0/0 interface. This IP serves as the default gateway for devices in LAN-1.
- **Activate the Interface** (`no shutdown`): Enables the interface, bringing it online to handle network traffic.
- **Exit Interface Configuration Mode** (`exit`): Returns to global configuration mode to configure the next interface.
- **Select Second Interface for Configuration** (`interface GigabitEthernet0/1`): Specifies the second interface (GigabitEthernet0/1) connected to Switch-2 (LAN-2).
- **Assign IP Address and Subnet Mask for Second Interface** (`ip address 192.168.1.100 255.255.255.0`): Assigns the IP address 192.168.1.100 with a subnet mask of 255.255.255.0 to the GigabitEthernet0/1 interface, making it the default gateway for LAN-2 devices.
- **Activate the Second Interface** (`no shutdown`): Enables the GigabitEthernet0/1 interface.
- **Exit Configuration Modes** (`exit`): Exits global configuration mode, returning to privileged EXEC mode.

```
enable                                  # Enter privileged EXEC mode
configure terminal                      # Enter global configuration mode
interface GigabitEthernet0/0            # Select interface GigabitEthernet0/0 for
                                                #configuration
ip address 10.10.10.100 255.255.255.0   # Assign IP address 10.10.10.100 and
                                          #subnet mask 255.255.255.0 to the interface
no shutdown                             # Activate the interface (bring it up)
exit                                    # Exit interface configuration mode
interface GigabitEthernet0/1
ip address 192.168.1.100 255.255.255.0
no shutdown
exit
```

Figure 8: CLI code for two network

Network Functionality

- **Inter-LAN Communication**: The router facilitates communication between LAN-1 (10.10.10.0/24) and LAN-2 (192.168.1.0/24) by routing packets between the two subnets. Devices in LAN-1 use 10.10.10.100 as their default gateway, while devices in LAN-2 use 192.168.1.100.
- **IP Addressing**: The IP addresses are assigned statically to ensure predictable communication. The subnet mask (255.255.255.0) indicates that each LAN supports up to 254 devices ($2^8 - 2$, excluding network and broadcast addresses).
- **Switches**: Switch-1 and Switch-2 operate at Layer 2, forwarding frames within their respective LANs. They connect the end devices (PCs and laptops) to the router.
- **Router Role**: The router operates at Layer 3, making forwarding decisions based on IP addresses to route traffic between the two LANs.

4.1.2 Router connection using interface

The network topology illustrates a router connecting two local area networks (LANs) through two switches (Switch0 and Switch1). LAN-1 comprises three devices—Laptop-PT0 (192.168.0.1), PC-PT0 (192.168.0.2), and Laptop-PT1 (192.168.0.3)—all within the 192.168.0.0/24 subnet, connected via Switch0 with the IP address 192.168.0.1 and subnet mask 255.255.255.0. LAN-2 includes three devices—PC-PT1 (192.168.1.1), Laptop-PT2 (192.168.1.2), and Laptop-PT3 (192.168.1.3)—within the 192.168.1.0/24 subnet, connected via Switch1 with the IP address 192.168.1.0 and subnet mask 255.255.255.0. The router interfaces are configured to enable communication between these LANs: the interface connected to Switch0 (LAN-1) is assigned the IP address 192.168.0.4, while the interface connected to Switch1 (LAN-2) is assigned the IP address 192.168.1.4. This setup ensures that the router acts as the default gateway for both LANs, facilitating inter-LAN communication by routing packets between the 192.168.0.0/24 and 192.168.1.0/24 subnets.

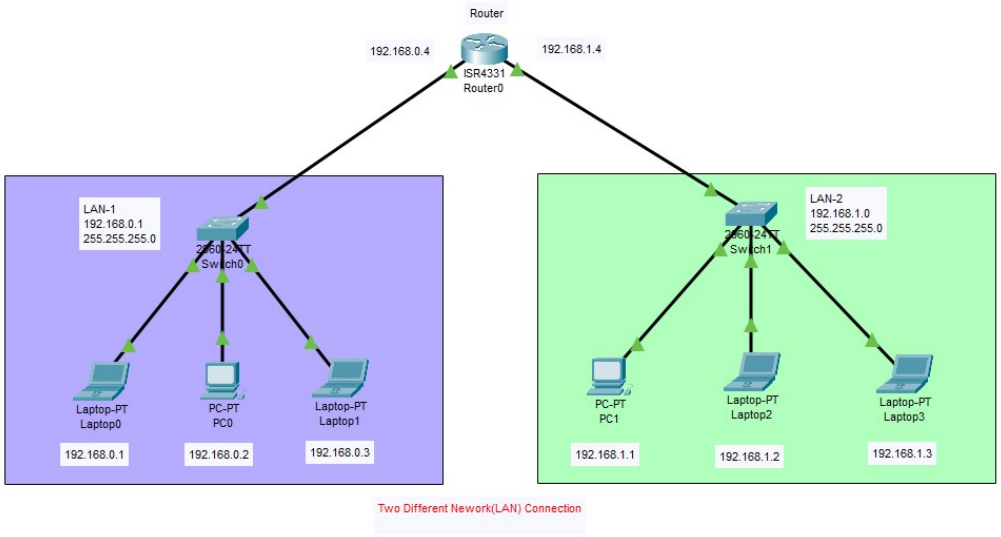

Figure 9: Router connection using interface

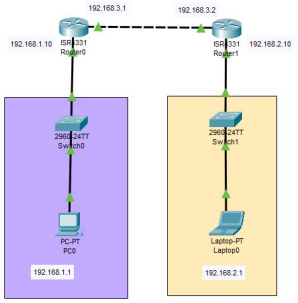

Figure 10: Basic Static Routing[2 Router,2 Switches,2 PC]

4.2 Basic Static Routing

Two routers connect two LANs using a 192.168.2.0/24 link (first router: 192.168.2.10, second router: 192.168.2.100). The first router (192.168.1.3) links to LAN-1 via a switch, serving PC-PT0 (192.168.1.1). The second router (192.168.3.2) connects to LAN-2 through another switch, serving Laptop-PT0 (192.168.2.1). Both LANs use a /24 subnet mask. The first router forwards packets from LAN-1 to the second router, which delivers them to LAN-2, enabling inter-LAN communication. Switches manage intra-LAN frame forwarding at Layer 2, while routers handle Layer 3 routing between the 192.168.1.0/24 and 192.168.2.0/24 subnets.

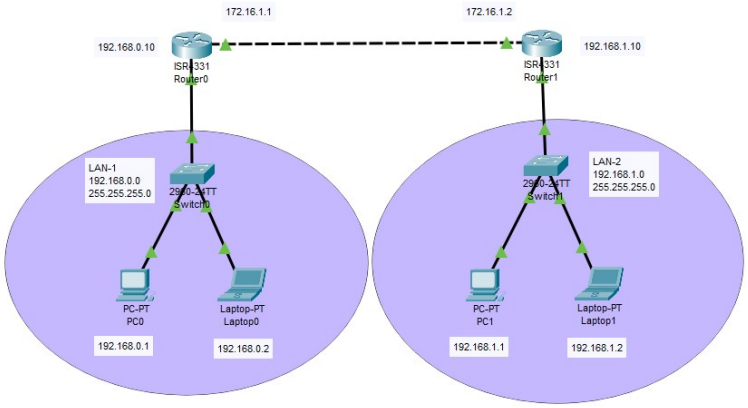

Figure 11: Static Routing

4.2.1 Static Routing

Static routing involves the manual configuration of routing tables within a router, where network administrators explicitly define the paths for network traffic instead of relying on dynamic routing protocols. This approach requires the administrator to specify the next hop IP address or outgoing interface for each destination network, creating fixed routes that do not automatically adjust to network topology changes.

In this figure [FIGURE 11] two routers connect two LANs via a 172.16.1.0/24 link (first router: 172.16.1.1, second router: 172.16.1.2). The first router (192.168.0.10) links to LAN-1 (192.168.0.0/24) through a switch, serving PC0 (192.168.0.1) and Laptop0 (192.168.0.2). The second router (192.168.1.10) connects to LAN-2 (192.168.1.0/24) via another switch, serving PC1 (192.168.1.1) and Laptop1 (192.168.1.2). Both LANs use a /24 subnet mask. The routers enable inter-LAN communication by routing packets between the 192.168.0.0/24 and 192.168.1.0/24 subnets, while switches handle intra-LAN frame forwarding at Layer 2.

4.2.2 Static Routing using CLI

The router configuration begins by entering privileged EXEC mode (enable) and global configuration mode (configure terminal). The first interface, GigabitEthernet0/0, is assigned IP 192.168.1.1/24 and activated (no shutdown). The second interface, GigabitEthernet0/1, gets IP 10.1.1.1/24 and is activated. A static route is set to reach the 10.1.1.0/24 network via 192.168.1.2 as the next hop. The configuration is verified using "show ip interface brief" to check interface status and IPs. Connectivity is tested by pinging 192.168.1.2, ensuring the router can communicate with the next-hop device in the network setup.

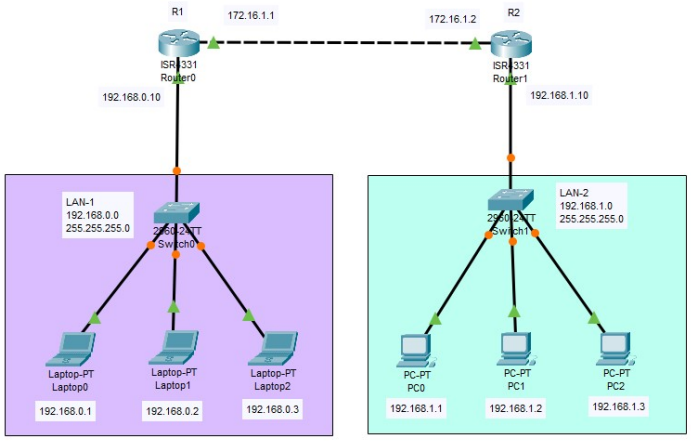

Figure 12: Static Routing- Connecting two network using CLI

```
enable                              # Enter privileged EXEC mode
configure terminal                  # Enter global configuration mode

# Configure interface GigabitEthernet0/0
interface GigabitEthernet0/0        # Select interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0   # Assign IP address to the interface
no shutdown                         # Activate the interface (bring it up)
exit                                # Exit interface configuration mode

# Configure interface GigabitEthernet0/1
interface GigabitEthernet0/1        # Select interface GigabitEthernet0/1
ip address 10.1.1.1 255.255.255.0   # Assign IP address to the second interface
no shutdown                         # Activate the interface (bring it up)
exit                                # Exit interface configuration mode

# Set a static route (if needed)
ip route 10.1.1.0 255.255.255.0 192.168.1.2  # Route to reach 10.1.1.0 network
                                             #via next-hop IP

# Check the status of interfaces
show ip interface brief             # Display status of interfaces and their IPs

# Test connectivity
ping 192.168.1.2                    # Test if the device can reach 192.168.1.2
```

Figure 13: CLI Code for two router

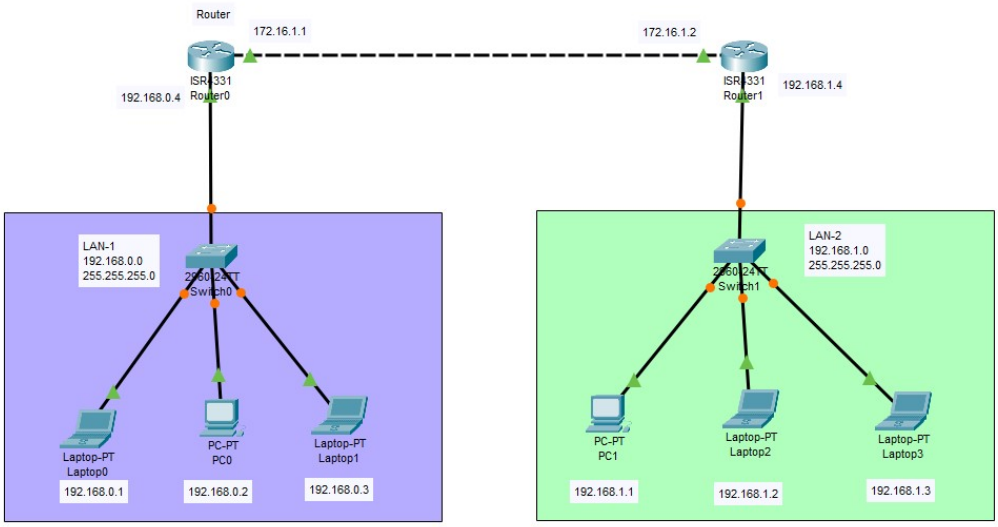

Figure 14: Static Routing Connecting Two network [2 Router, 2 LAN]

4.2.3 Static Routing-Connecting Two Network [2 Router, 2 LAN]

Connecting two networks using static routing with two routers and two LANs involves manually configuring each router's routing table to direct traffic between the different LAN subnets, specifying the next hop router for destination networks.

The network topology features two routers connecting two LANs through a 172.16.1.0/24 link (first router: 172.16.1.1, second router: 172.16.1.2). The first router (192.168.0.4) connects to LAN-1 (192.168.0.0/24) via a switch, supporting Laptop0 (192.168.0.1), PC0 (192.168.0.2), and Laptop1 (192.168.0.3). The second router (192.168.1.4) links to LAN-2 (192.168.1.0/24) through another switch, serving PC (192.168.1.1), Laptop2 (192.168.1.2), and Laptop3 (192.168.1.3). Both LANs use a 255.255.255.0 subnet mask, allowing up to 254 devices per LAN. The routers enable inter-LAN communication by routing packets between the 192.168.0.0/24 and 192.168.1.0/24 subnets. For example, a packet from Laptop0 to Laptop2 is sent to the first router (192.168.0.4), which forwards it via the 172.16.1.0/24 link to the second router (192.168.1.4) for delivery to LAN-2. The switches operate at Layer 2, managing intra-LAN frame forwarding using MAC addresses, ensuring efficient communication within each LAN. The routers, functioning at Layer 3, handle IP-based routing, making forwarding decisions to connect the two subnets. This setup ensures seamless data exchange between devices in different LANs, demonstrating a fundamental inter-LAN routing configuration suitable for small-scale networks.

Three laptops are connected to the switch. They are assigned IP addresses 192.168.0.1, 192.168.0.2, and 192.168.0.3 respectively, all within the 192.168.0.0 subnet. The router's interface connected to the switch has an IP address of 192.168.0.10.

The right side of the image shows the configuration interface for Router0, specifically the static routing settings. A static route is configured to forward traffic destined for the network 192.168.1.0/24 via the next hop IP address 172.16.1.2. This configuration enables communication between devices within LAN-1 and networks reachable through the router's other interface.

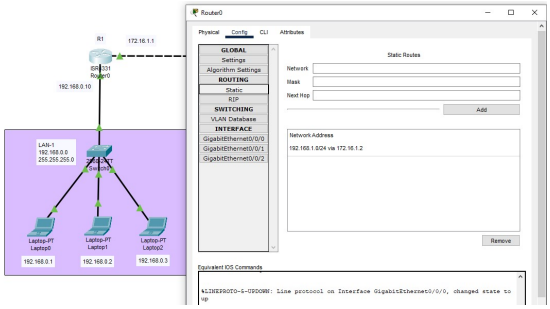

Figure 15: Router1 Config

5 RIP Routing (Day 05)

RIP (Routing Information Protocol) is a straightforward distance-vector routing protocol where routers periodically broadcast their entire routing tables to directly connected neighbors. It relies on hop count as the primary metric to determine the best path, with a limit of 15 hops. While easy to configure and suitable for small networks, RIP suffers from slow convergence during topology changes and uses broadcast updates in its first version, making it less efficient for larger, more dynamic environments compared to modern routing protocols.

This network configuration features two separate Local Area Networks, LAN-1 and LAN-2, interconnected via two routers. LAN-1, operating on the 192.168.0.0 subnet, connects its devices through a switch to Router0, which serves as its gateway with the IP address 192.168.0.4. Similarly, LAN-2, utilizing the 192.168.1.0 subnet, connects its devices through another switch to Router1, acting as its gateway with the IP address 192.168.1.4. The crucial link between these two LANs is established by the direct connection between Router0 and Router1, with their respective interfaces configured on the 172.16.1.0 subnet (172.16.1.1 for Router0 and 172.16.1.2 for Router1). This interconnected router setup enables the routing of network traffic between the distinct IP subnets of LAN-1 and LAN-2. Overall:

- **LAN-1:** Network 192.168.0.0, connected to Router0 (IP 192.168.0.4).
- **LAN-2:** Network 192.168.1.0, connected to Router1 (IP 192.168.1.4).
- **Router Interconnection:** Router0 (IP 172.16.1.1) connected to Router1 (IP 172.16.1.2).
- **Functionality:** Enables communication between devices in LAN-1 and LAN-2 through routing.

In the figure 17 a network topology featuring a single router (Router0) connected to one Local Area Network (LAN-1). LAN-1 operates on the 192.168.0.0 subnet and utilizes a switch (Switch0) to connect multiple end devices, including laptops and a PC, with IP addresses in the 192.168.0.x range. Router0 has an interface with the IP address 192.168.0.4, serving as the gateway for devices within LAN-1. Additionally, Router0 has another interface with the IP address 172.16.1.1, which appears to be connected to an external network or another router (labeled simply as "Router" with IP 172.16.1.1, which is likely a representation of a broader network). The configuration window for Router0 shows settings for RIP routing, indicating that the network might be configured to dynamically learn routes using this protocol.

Summary:

- **Single Router (Router0):**
  - Interface in LAN-1: IP address 192.168.0.4.

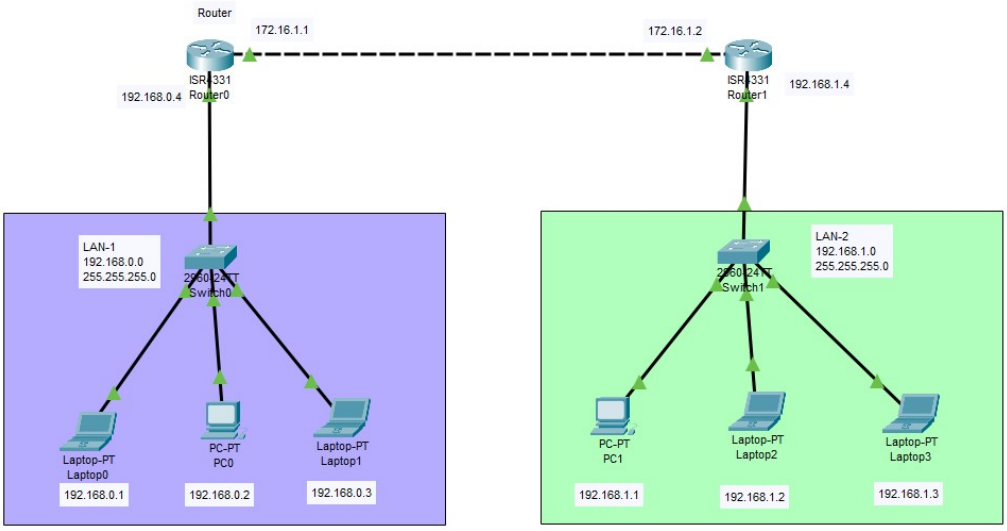

Figure 16: RIP Routing

  - Interface to external network/another router: IP address 172.16.1.1.

- **One LAN (LAN-1):**
  - Network address: 192.168.0.0.
  - Connected to Router0 via Switch0.
  - Includes devices with IP addresses 192.168.0.1, 192.168.0.2, and 192.168.0.3.
- **External Connection:** Router0 connected to a network/router with IP address 172.16.1.1.
- **RIP Configuration:** Router0's configuration shows settings for RIP routing.

In figure 17 a network with a single router, Router1, connected to a Local Area Network, LAN-2. LAN-2 operates on the 192.168.1.0 subnet, connecting two laptops (Laptop2 and Laptop3) through a switch (Switch1). These laptops have IP addresses within the 192.168.1.x range. Router1 has an interface with the IP address 192.168.1.4, serving as the gateway for LAN-2. Additionally, Router1 has another interface with the IP address 172.16.1.2, suggesting a connection to an external network or another router. The configuration window for Router1 shows that RIP routing is enabled and configured for the 172.16.0.0 and 192.168.1.0 networks, indicating that Router1 is advertising these networks to its RIP neighbors and learning routes to other networks.

Bullet Point Summary:

- **Single Router (Router1):**
  - Interface in LAN-2: IP address 192.168.1.4.
  - Interface to external network/another router: IP address 172.16.1.2.
- **One LAN (LAN-2):**
  - Network address: 192.168.1.0.
  - Connected to Router1 via Switch1.

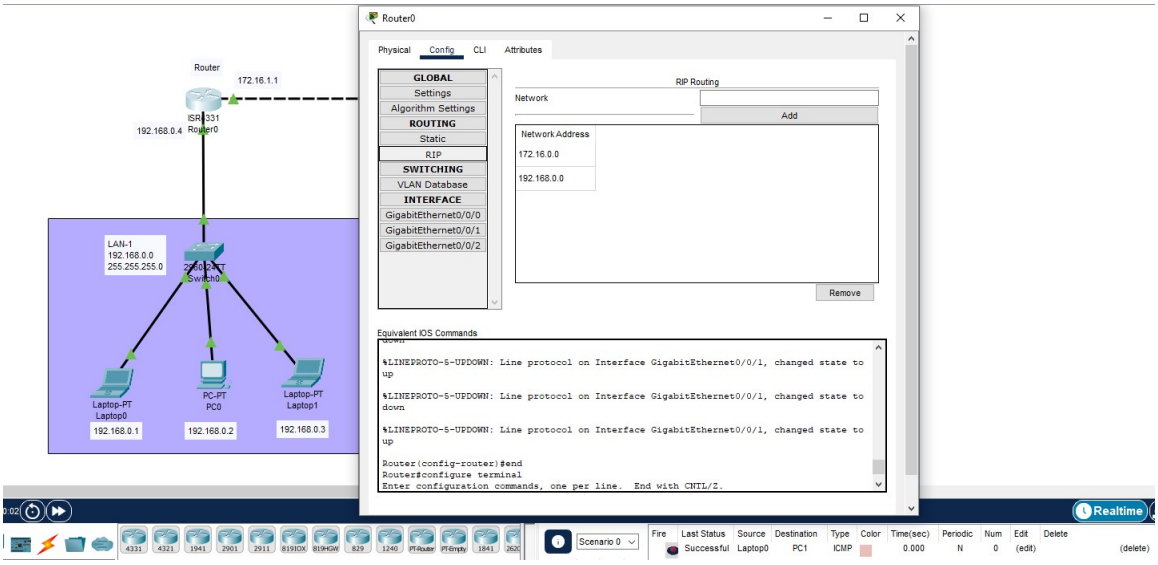

Figure 17: Router 1 config

  - Includes laptops with IP addresses 192.168.1.2 and 192.168.1.3.

- **RIP Configuration on Router1:**
  - RIP enabled.
  - Advertising networks: 172.16.0.0 and 192.168.1.0.
- **External Connection:** Router1 connected to a network/router with IP address 172.16.1.2.

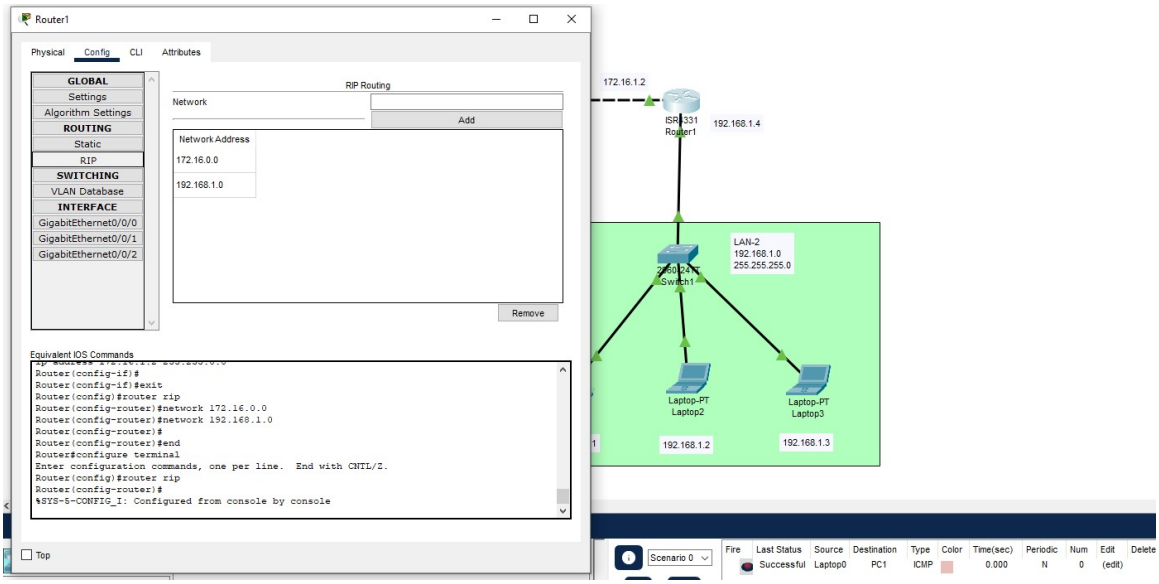

Figure 18: Router 2 Config

6 DNS, DHCP and Web server (DAY 07)

DNS (Domain Name System): Imagine trying to remember a long string of numbers for every website you visit. The Domain Name System solves this by acting as a crucial translator on the internet. When you type a web address like "example.com" into your browser, DNS servers work behind the scenes to look up the corresponding numerical IP address (e.g., 192.0.2.44) associated with that domain name. This translation process allows your computer to connect to the correct web server hosting the website. Without DNS, navigating the internet would be incredibly cumbersome, requiring users to memorize and enter complex IP addresses for every online destination. It's a hierarchical and distributed system that ensures the efficient and user-friendly functioning of the World Wide Web.

DHCP (Dynamic Host Configuration Protocol): Managing IP addresses manually for every device on a network can be a tedious and error-prone task. DHCP simplifies this process significantly. When a DHCP-enabled device joins a network, it automatically requests network configuration information from a DHCP server. The server then dynamically assigns an available IP address, along with other essential details like the subnet mask, default gateway, and DNS server addresses. This automated allocation prevents IP address conflicts, reduces administrative overhead, and makes it easy to add or remove devices from a network. DHCP ensures that devices can seamlessly connect and communicate on the network without requiring manual configuration by a network administrator or the user.

Web Server: At its core, a web server is a computer system designed to store, process, and deliver website content to users. When you access a website, your web browser sends a request to the web server hosting that site. The server then responds by sending back the necessary files, such as HTML documents, CSS stylesheets, JavaScript files, images, and videos, which your browser then renders to display the webpage. Web servers utilize protocols like HTTP (Hypertext Transfer Protocol) to communicate with web browsers. They can range from simple software running on a personal computer to powerful hardware managing high-traffic websites. Popular web server software includes Apache and Nginx, which handle requests efficiently and ensure the reliable delivery of web content to users across the internet.

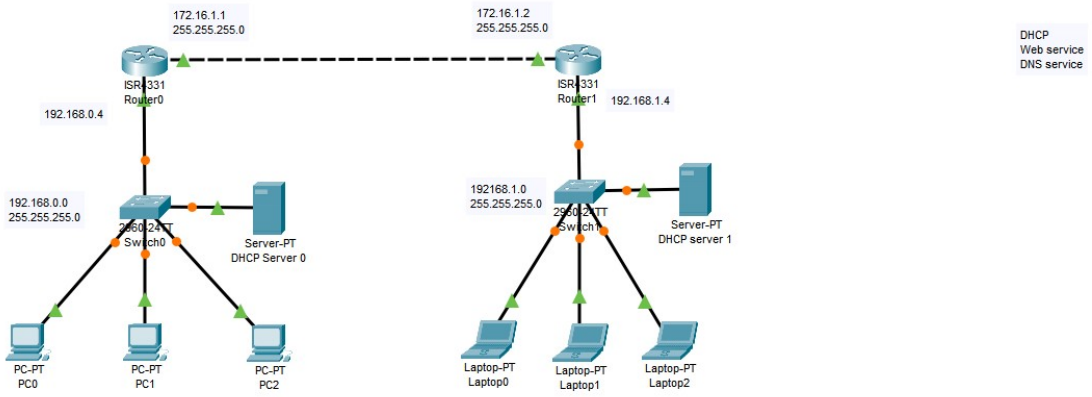

Figure 19: DNS, DHCP Web server

DHCP (Dynamic Host Configuration Protocol):
In this network, we see two dedicated servers labeled "DHCP Server 0" and "DHCP Server 1".

- **DHCP Server 0:** Located on the left side, connected to Switch0 within the 192.168.0.0 network. This server is likely configured to provide IP addresses and other network configuration (like gateway and DNS server addresses) to the PCs (PC0, PC1, PC2) connected to Switch0. When these PCs boot up or request an IP address, they would contact DHCP Server 0 to obtain their necessary network settings automatically.
- **DHCP Server 1:** Located on the right side, connected to Switch1 within the 192.168.1.0 network. Similarly, this server is probably configured to provide IP addresses and network configuration to the laptops (Laptop0, Laptop1, Laptop2) connected to Switch1. These laptops would automatically receive their IP addresses and other settings from DHCP Server 1.

The presence of separate DHCP servers on each LAN segment allows for localized and efficient IP address management within those segments.

DNS (Domain Name System):

While there isn't a server explicitly labeled "DNS Server" in the diagram, the note in the top right corner indicates "DHCP Web service DNS service" are likely functionalities provided within this network.

- It's possible that one or both of the "Server-PT" devices are also configured to act as DNS servers. The DHCP servers would then distribute the IP address(es) of these DNS servers to the client devices (PCs and laptops) when they receive their IP configurations.
- Alternatively, the routers (Router0 and/or Router1) might be configured to handle basic DNS forwarding, relaying DNS queries to an external DNS server.

Without explicitly labeled DNS servers, we infer their presence and function based on the note, suggesting that name resolution (translating website names to IP addresses) is a service available within this network.

Web Server:

Similar to the DNS service, there isn't a server explicitly labeled "Web Server". However, the note "DHCP Web service DNS service" implies that web services are also available.

- It's probable that one or both of the "Server-PT" devices are also hosting web server software. Users on the PCs and laptops could then access web pages hosted on these servers using a web browser.
- The "Web service" could also refer to the management interfaces of the routers or switches, accessible via a web browser for configuration purposes.

Again, based on the note, we understand that the capability to host and serve web content is likely present within this network, potentially residing on one or both of the generic "Server-PT" devices.

In summary, this network utilizes dedicated DHCP servers for automatic IP address assignment within each LAN. While not explicitly labeled, DNS and web services are also indicated as available, likely hosted on the generic "Server-PT" devices, enabling name resolution and the serving of web content to the connected clients. The routers facilitate connectivity between the LANs and potentially to external networks.