**Assignment Module: 5**

**Section 1: Multiple Choice**

1. What is the primary function of a router in a computer network?

Answer: Forwarding data packets between networks.

2. What is the purpose of DHCP (Dynamic Host Configuration Protocol) in a

computer network?

Answer: Dynamically assigning IP addresses to devices.

3. Which network device operates at Layer 2 (Data Link Layer) of the OSI model

and forwards data packets based on MAC addresses?

Answer:  Switch.

4. Which network topology connects all devices in a linear fashion, with each

device connected to a central cable or backbone?

Answer: Bus.

**Section 2: True or False**

5. A VLAN (Virtual Local Area Network) allows network administrators to logically segment a single physical network into multiple virtual networks, each with its own broadcast domain.

Answer: True.

6.TCP (Transmission Control Protocol) is a connectionless protocol that provides reliable, ordered, and error-checked delivery of data packets over a network.

Answer: False.

Reason: TCP is not a connectionless protocol; it is a connection-oriented protocol. It establishes a connection between communicating devices before data transmission begins, ensuring reliable, ordered, and error-checked delivery of data packets. This contrasts with connectionless protocols like UDP, which do not establish a connection and may not guarantee delivery or order.

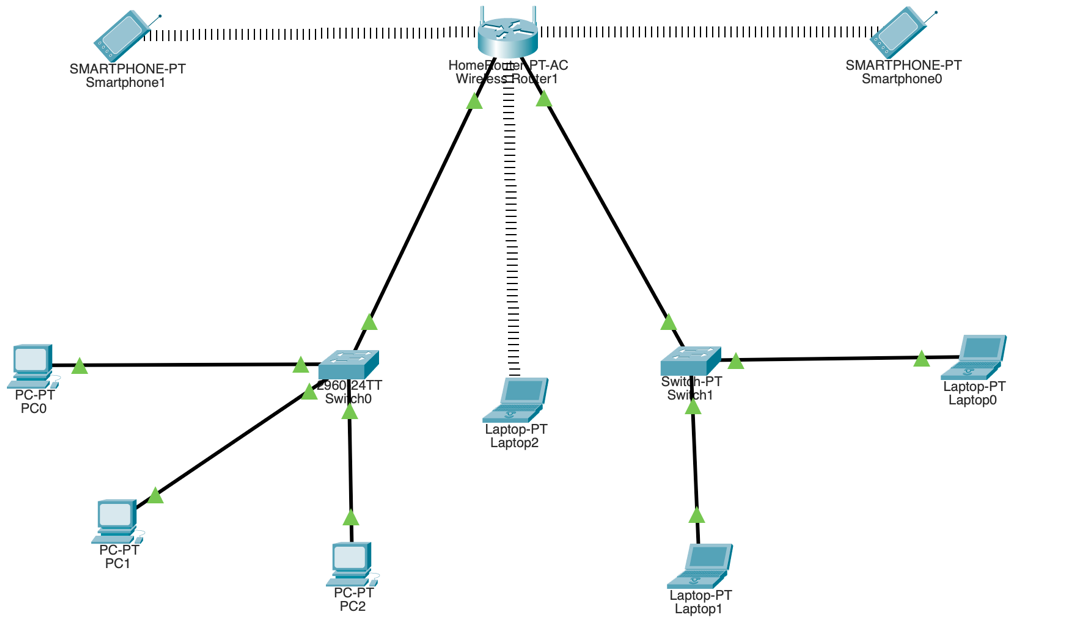
7. A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Answer: True.

**Section 3: Short Answer**

8. Describe the steps involved in setting up a wireless network for a small

office or home office (SOHO) environment.

Answer:

**Equipment Used for SOHO Environment:**

**Wireless Router**: Ensure you have a wireless router that supports your internet speed.

**Ethernet Cable:** To connect the router to the Switches, PCs and Laptops.

**Laptop:** The device you want to connect wirelessly.

**Steps to Set Up the Wireless Network:**

1. **Step 1: Internet Connectivity via Wireless Router**

The Wireless Router acts as the central networking device. It likely connects to an external ISP (not shown) for internet access. It provides both wired Ethernet ports and wireless signals.

1. **Step 2: Switches Connected to the Router**

Switch0 and Switch1 are connected to the LAN ports of the wireless router using Ethernet cables. The router provides IP addressing (via DHCP) and internet access to all connected devices.

**Step 3: Wired Devices Connected to Switches**

Switch connects to three PCs: PC0, PC1, and PC2

Switch2 connects to four Laptops:

LP1, LP0, and one port back to the router

These switches extend the wired connectivity and help in LAN communication among all devices.

**Step 4: Wireless Devices**

Laptop2, Smartphone0 and Smartphone1connect to the wireless signals broadcasted by the router. They do not need Ethernet cables but must be within range of the Wi-Fi router. These devices receive IP addresses from the router and can access the internet and other LAN devices.

**Step 5: DHCP and IP Addressing**

The router acts as the DHCP server, assigning IP addresses dynamically to all devices wired and wireless. All devices are likely part of the same subnet (e.g., 192.168.0.1), allowing communication across the network.

**Step 6: Communication Between Devices**

Devices connected to the same switch or different switches can communicate via the router's LAN.

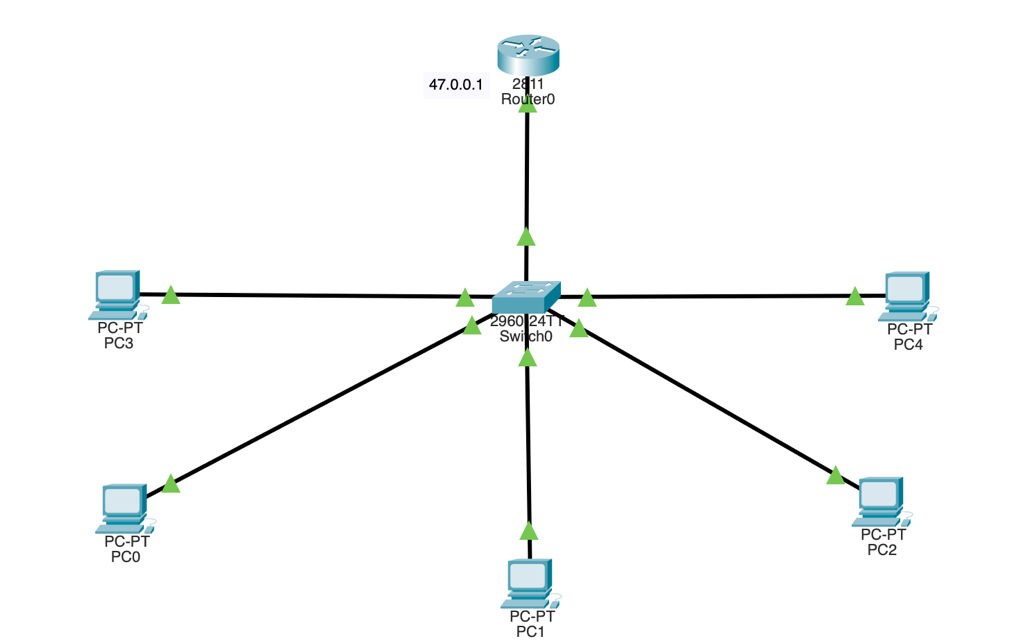
Wireless and wired devices are part of the same LAN, enabling file sharing, printer access, and internet use.

**Section 4: Practical**

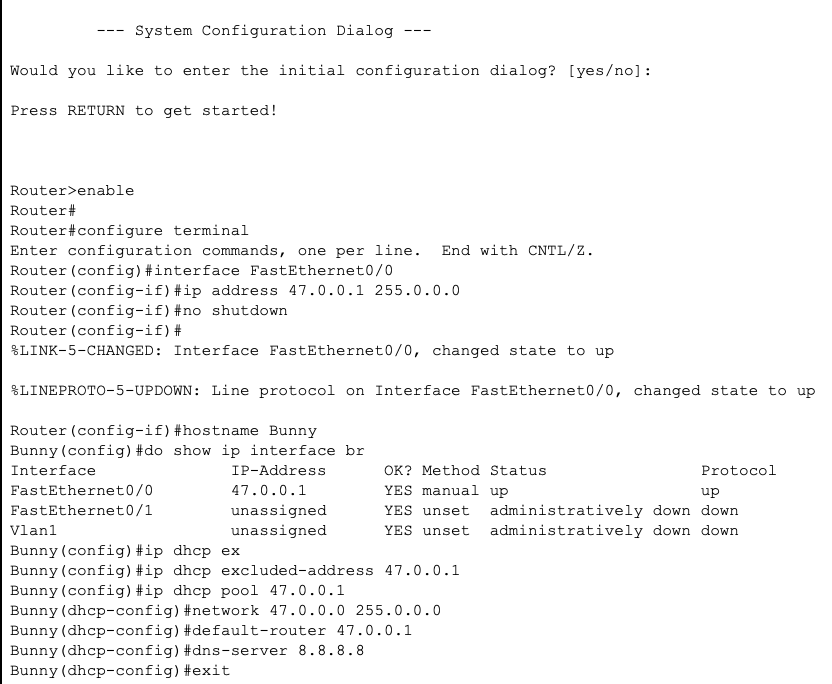
9. Demonstrate how to configure a router for Internet access using DHCP (Dynamic Host Configuration Protocol).

Answer:

1. Connect your router to a network devices like switch and Pcs.

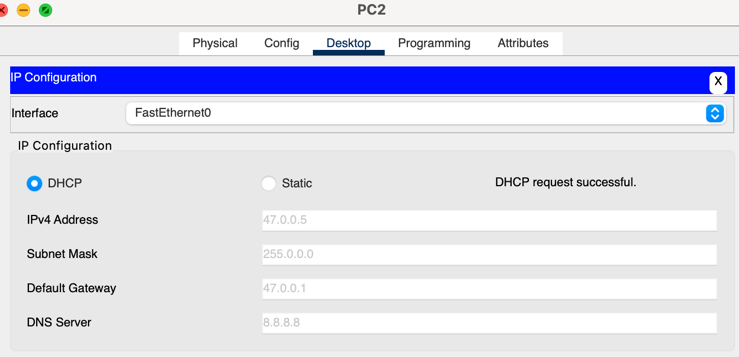


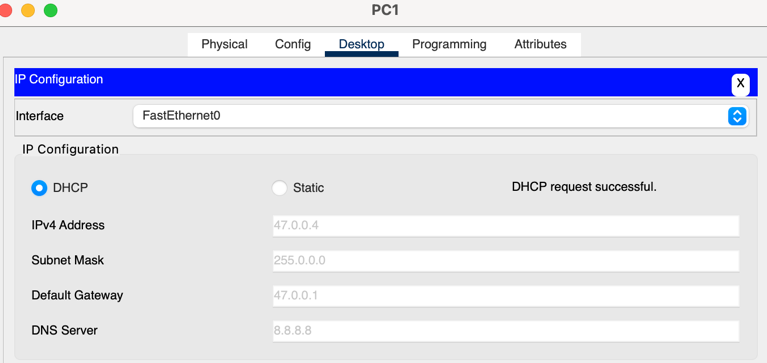
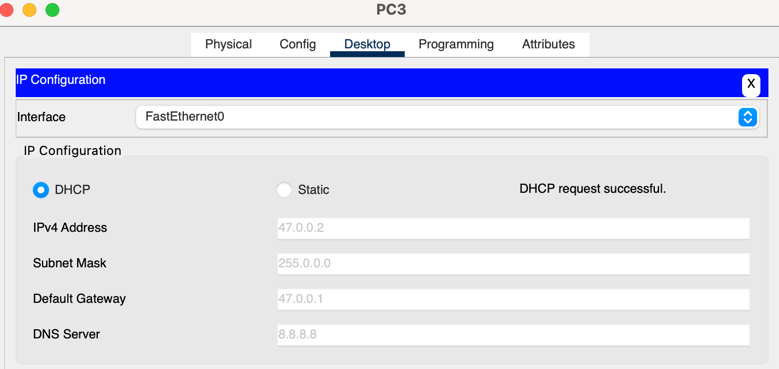
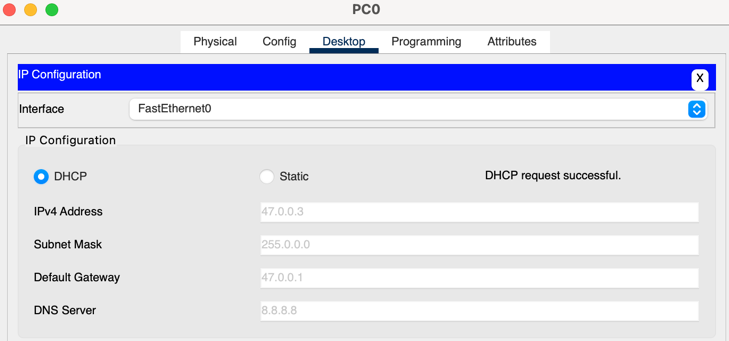
1. Click on the router to access its configuration interface and navigate to the CLI (Command Line Interface).



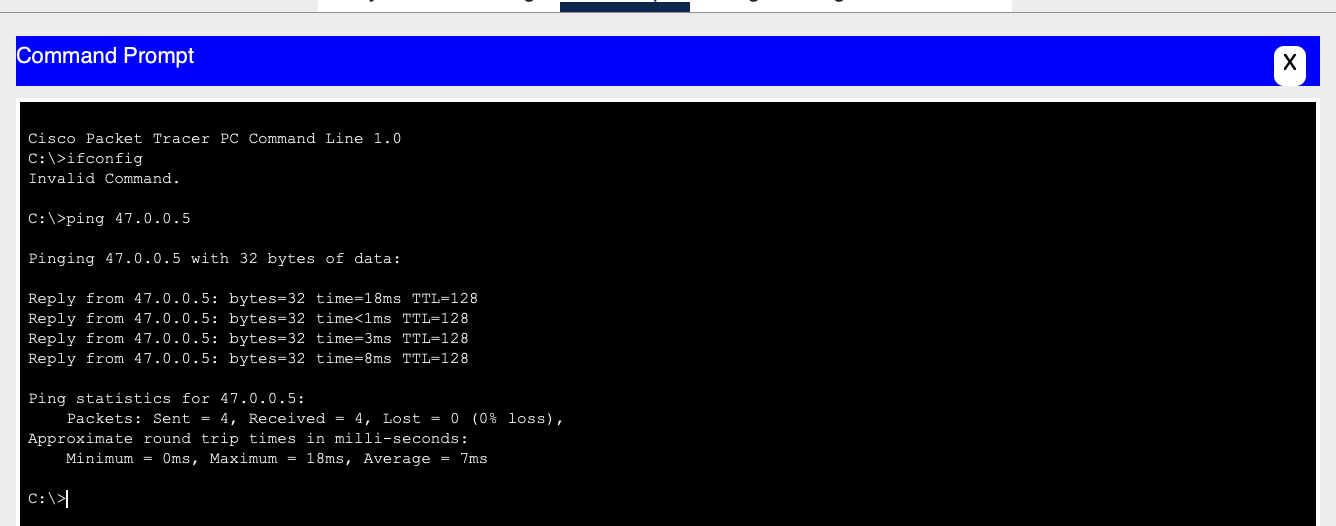
**Configuration Steps of DHCP:**

1. First give a router a static IP address and turn on the router.
2. Router > Enable
3. Router#
4. Router # Config terminal
5. Router (config)# interface Fast Ethernet 0/0
6. Router (config-if) #ip address 47.0.0.1 255.0.0.0
7. Router (config-if) # no shutdown
8. Router (config-if) #hostname Bunny
9. Bunny (config-if) #do show ip interface br
10. Bunny (config-if) #ip dhcp ex (Press Tab)
11. Bunny (config-if) #ip dhcp excluded-address 47.0.0.1
12. Bunny (config-if) #ip dhcp pool 47.0.0.1
13. Bunny(dhcp-config) # network 47.0.0.0 255.0.0.0
14. Bunny(dhcp-config) # default-router 47.0.0.1
15. Bunny (dhcp-config) #dns-server 8.8.8.8
16. Bunny (dhcp-config) #exit
17. After successful configuration we can assign the DHCP IP address to all the network devices.





1. After assign the IP address to network devices, open the terminal and see the if data packets are sent or not.



**Section 5: Essay**

10. Discuss the importance of network documentation in the context of building and managing networks.

**Answer:** Network documentation is crucial for building and managing networks. It provides a clear blueprint of the network, including its physical and logical components, configurations, and connections, which is essential for efficient troubleshooting, seamless upgrades, and effective network management. Proper documentation ensures that all team members are on the same page, leading to better communication, informed decision-making, and streamlined operations.

**Here's why network documentation is so important:**

1. **Troubleshooting and Maintenance**:

**Faster Problem Resolution:** When a network issue arises, having clear documentation allows technicians to quickly identify the root cause and implement a solution, minimizing downtime.

**Reduced Mean Time to Repair (MTTR):** Detailed documentation helps in diagnosing and resolving faults faster, reducing the time it takes to restore network functionality.

**Historical Record:** Documentation provides a historical record of changes,

configurations, and troubleshooting steps, which is invaluable for identifying recurring problems and preventing future occurrences.

**2. Network Management and Planning:**

**Improved Visibility:** Network documentation provides a comprehensive view of the network infrastructure, allowing administrators to understand how data flows, where security measures are implemented, and how different components interact.

**Efficient Upgrades and Expansion:** Documentation helps in planning and implementing network upgrades and expansions by providing a clear understanding of the existing infrastructure and its limitations.

**Informed Decision-Making:** With comprehensive documentation, network administrators can make informed decisions about resource allocation, security policies, and future investments.

**Compliance:** Network documentation is often a requirement for meeting regulatory compliance standards such as PCI DSS and GDPR, which govern data protection and privacy.

**3. Knowledge Sharing and Onboarding:**

**Preserves Institutional Knowledge:** Documentation ensures that critical knowledge about the network is not lost when employees leave or change roles.

**Facilitates Onboarding:** New team members can quickly learn about the network and its intricacies through well-documented resources, reducing the time it takes to become productive.

**Cross-Training:** Documentation promotes knowledge sharing among team members, enabling them to understand different aspects of the network and contribute to its overall management.

**4.** **Automation and Scalability:**

**Enables Automation:** Well-documented networks can be more easily automated, leading to increased efficiency and reduced manual effort.

**Supports Scalability:** Accurate documentation helps in scaling the network to accommodate growing business needs, as it provides a clear roadmap for adding new devices, services, or locations.

In essence, network documentation is not just a nice-to-have; it's a fundamental aspect of building and managing robust, reliable, and secure networks. It's an investment that pays off in terms of reduced downtime, improved efficiency, and enhanced overall network performance.