### Problem Statement: Network Setup and Configuration for a Small Tech Business

#### \*\*Background:\*\*

You are the IT administrator for a small tech startup that is setting up a new office. The office has multiple devices, including laptops, tablets, and smartphones that need to be connected to the internet and communicate with each other efficiently. The office also requires a DHCP server to manage IP address allocation dynamically. Your task is to design and configure the network infrastructure that will support these needs, ensuring reliable connectivity both internally and to the internet.

#### \*\*Scenario:\*\*

Your company has just moved into a new office space. The office layout is such that different teams work in different areas, requiring wireless access points to ensure coverage throughout the office. The company also needs to ensure that all devices can connect to the internet seamlessly while maintaining internal communication for file sharing, printing, and collaboration.

#### \*\*Network Requirements:\*\*

1. \*\*Internet Connectivity:\*\*

- Ensure all devices have reliable access to the internet.

- Establish a secure connection between the office network and the internet service provider.

2. \*\*Internal Communication:\*\*

- Allow all devices (laptops, tablets, smartphones) to communicate within the internal network.

- Configure a switch to connect wired devices and access points for wireless devices.

3. \*\*Dynamic IP Address Allocation:\*\*

- Set up a DHCP server to automatically assign IP addresses to devices within the office network to simplify management.

4. \*\*Wireless Network Setup:\*\*

- Deploy and configure three wireless access points (WAPs) with the following configurations:

- \*\*WAP 1\*\*: No authentication (Open Network), supporting only 2.4 GHz frequency.

- \*\*WAP 2\*\*: Secured with WEP, supporting both 2.4 GHz and 5 GHz frequencies.

- \*\*WAP 3\*\*: Secured with WPA2-PSK, supporting both 2.4 GHz and 5 GHz frequencies.

5. \*\*Network Security:\*\*

- Implement a basic level of network security to protect internal data from unauthorized access.

- Ensure that the internal network is isolated from external threats.

#### \*\*Task:\*\*

Using the provided network topology diagram, your job is to:

1. \*\*Configure the Cable Modem and Router\*\*:

- Connect the router to the modem using the `172.168.1.x` IP range to establish a link with the internet.

- Set the router's internal IP address to `192.168.1.1` to act as the gateway for the internal network.

2. \*\*Set Up the Switch\*\*:

- Connect the router to the switch to facilitate communication between all devices within the local network.

3. \*\*Deploy and Configure Access Points\*\*:

- Position and configure three wireless access points (APs) as follows:

- \*\*Access Point 1\*\*: Configure as an open network (no authentication), operating on the 2.4 GHz band.

- \*\*Access Point 2\*\*: Secure with WEP encryption, supporting both 2.4 GHz and 5 GHz bands.

- \*\*Access Point 3\*\*: Secure with WPA2-PSK encryption, supporting both 2.4 GHz and 5 GHz bands.

- Assign appropriate IP addresses within the `192.168.1.x` range.

4. \*\*Install and Configure the DHCP Server\*\*:

- Ensure the DHCP server is operational and configured to allocate IP addresses dynamically within the `192.168.1.x` range.

5. \*\*Test Connectivity\*\*:

- Verify that all devices (laptops, tablets, smartphones) can connect to the internet and communicate with each other.

- Ensure devices receive IP addresses automatically from the DHCP server.

- Test the three different wireless networks to confirm they are functioning as intended with their respective security settings and frequencies.

#### \*\*Expected Outcome:\*\*

By the end of this task, your network should be fully operational, with all devices connected to the internet and capable of internal communication. The DHCP server should be managing IP addresses effectively. The three wireless networks should provide different levels of security and frequency options as required, catering to various devices and usage scenarios within the office. The network should also be secure from external threats.

This setup will be presented to the business stakeholders as a demonstration of the company's technical capabilities and preparedness for a smooth operational start.