

# Problem Statement: IoT-Enabled Smart Office Setup for a Small Tech Business

## Background:

You are the IT administrator for a small tech business aiming to create a smart office environment by leveraging IoT (Internet of Things) technology. This includes the integration of smart appliances, environmental controls, and security devices into a centralized network. The objective is to provide efficient management, control, and monitoring of all IoT devices through a secure network.

## Scenario:

The office environment includes multiple IoT devices connected via wireless access points (WAPs) and controlled using a central IoT server. A smartphone acts as the primary interface to manage the devices. Specific configurations for WAPs and the IoT server are required for seamless and secure integration.

---

## Network and Device Requirements:

### 1. Wireless Access Points (WAPs):

- **SSID and Authentication Setup:**

- WAP 3:

- **SSID:** IoT\_WAP

- **Authentication:** WPA2-PSK (PSK Pass Phrase: qwertyuiop)

- **Frequency:** 2.4 GHz and 5 GHz

- Ensure all IoT devices use the same SSID and corresponding authentication method for connection.

### 2. IoT Server Configuration:

- **Server Role:** Acts as the DHCP server and IoT registration hub.

- **IP Address:** 192.168.1.5

- **IoT Device Registration:**

- Use the IoT server interface for device registration.
  - Login credentials: Initially **admin** for both username and password.
  - Create a dedicated **IoT administrator account** with a username (e.g., **iotadmin**) and a secure password for device management.

### 3. Smartphone Integration:

- **Setup for Access:**

- Use the smartphone to connect to the IoT\_WAP SSID.
  - Navigate to the IoT Server's web interface (192 . 168 . 1 . 5).
  - Use the created administrator credentials to log in to the server.

- **IoT Monitoring:**

- Register IoT devices through the smartphone interface.
  - Access and control devices via the IoT Monitor Admin page.

### 4. IoT Device Integration:

- Devices include:
  - Smart appliances: Fan, air conditioner, coffee machine, humidifier.

- Environmental controls: Thermostat, desk lamp.
- Security devices: Webcam, siren, garage door, window sensors.
- Utility sensors: Water drain sensor.
- Ensure devices are configured to use the same SSID (IoT\_WAP) and authentication method.

#### 5. Network Infrastructure:

- **Router (192 . 168 . 1 . 1):** Acts as the gateway for internet and external communication.
- **Switch:** Connects all wired components, including the server and access points.
- **WAPs:** Extend wireless coverage for IoT devices.

#### 6. Network Security:

- Test and secure each access point.
  - Ensure unauthorized devices cannot connect to the network.
  - Enforce encryption for WAPs with authentication enabled.
- 

### Steps to Demonstrate the Setup:

#### 1. WAP Configuration:

- Configure each access point with its respective SSID, authentication method, and frequency bands as shown in the WAP setup image.

#### 2. Server Setup:

- Set the IoT server's IP address to 192 . 168 . 1 . 5 and enable DHCP.
- Register devices through the smartphone interface by creating a dedicated IoT admin account.

#### 3. Device Connection:

- Connect each IoT device to the WAP corresponding to its configuration.
- Verify device registration on the IoT server.

#### 4. Smartphone Control:

- Use the smartphone to log in to the IoT server and access the IoT Monitor.
  - Demonstrate real-time control and monitoring of connected devices.
- 

### Expected Outcome:

The smart office network will be fully operational, with all IoT devices registered on the server and accessible via the smartphone interface. WAPs will provide secure and reliable connectivity for IoT devices. The demonstration will showcase how IoT technology can enhance automation, security, and efficiency in a small tech business environment.