**3.11.1 Packet Tracer - Network Security Exploration - Physical Mode**

**📌 Overview**

This lab explores network security in different environments, including a **Data Center, ISP, Coffee Shop, and Home Network**, using **Cisco Packet Tracer Physical Mode (PTPM)**. It focuses on **IoT security, VPN implementation, WLAN security, and MAC filtering**.

**🔹 Objectives**

**Part 1: Explore the Networks**

* Investigate the **Data Center**, **ISP**, **Coffee Shop**, and **Home** networks.
* Identify the **network infrastructure** and connected devices.
* Examine **access lists**, **IoT configurations**, and **network security settings**.

**Part 2: Implement Security Measures**

* **Configure IoT security** (Smoke Detector in the Data Center).
* **Secure Public Wi-Fi using a VPN** (Coffee Shop VPN Laptop).
* **Set up secure WLANs in Home Network** (HomeNet & GuestNet with MAC filtering).

**🔹 Part 1: Network Exploration**

**1️⃣ Data Center Exploration**

✅ **Key Findings:**

* **Router in Wiring Closet:** DC1\_R1
* **Connection to ISP:** Fiber Cable
* **NAT Translation Device:** DC\_Edge-Rtr1
* **Access List Applied on:** g0/0/0 (Inbound)
* **IoT Security Devices:** Monitored doors, sirens, humidity & temperature sensors

**2️⃣ Coffee Shop Network Exploration**

✅ **Key Findings:**

* **Clients Connection:** Wireless (Wi-Fi)
* **Internet Connection:** Coaxial Cable
* **Devices:** Router, Cable Modem, WLAN Controller, 2 APs
* **IP Addresses:** 192.168.0.11, 192.168.0.12

**3️⃣ Home Network Exploration**

✅ **Key Findings:**

* **ISP Connection:** Cable Modem
* **Connected Devices:** Router, 2 Laptops, 2 Wired PCs

**🔹 Part 2: Implementing Security Measures**

**1️⃣ Configuring IoT Smoke Detector in Data Center**

✅ **Steps Taken:**

1. **Set Device Name:** Smoke Detector-DC1
2. **Enabled DHCP for Gateway/DNS**
3. **IoT Server Address:** 172.31.0.2
4. **Wi-Fi Security:** SSID: DC\_WLAN, WPA2-PSK, Passphrase: ciscorocks
5. **Registered Device**

**2️⃣ Configuring VPN in Coffee Shop**

✅ **Steps Taken:**

1. **Connected VPN Laptop** (IP: 192.168.0.12)
2. **Pinged VPN Server (10.0.0.2)**
3. **VPN Configuration:**
   * GroupName: REMOTE, GroupKey: CISCO
   * Server IP: 10.0.0.2, Username: VPN, Password: ciscorocks
4. **VPN Connected Successfully!**
5. **FTP File Transfer Over VPN:** PTsecurity.txt

**3️⃣ Securing WLANs in Home Network**

✅ **Steps Taken:**

1. **Router Configuration:**
   * IP: 192.168.0.254, DHCP: Enabled, DNS: 10.2.0.125
2. **WLANs Configured:**
   * HomeNet: Hidden, WPA2-PSK, Pass: ciscorocks
   * GuestNet: Visible, WPA2-PSK, Pass: guestpass
3. **MAC Filtering Enabled:**
   * Home Laptop: 00:01:42:2B:9E:9D
   * Guest Laptop initially blocked, later added
4. **Successfully Connected Home & Guest Laptops!**

**🔹 Security Measures Used**

✅ **Implemented Security Techniques:**

* **IoT Security:** Environmental & physical protection
* **VPN Security:** Encrypted public Wi-Fi traffic
* **WLAN Security:** WPA2-PSK, MAC Filtering
* **Access Lists:** Restricted unauthorized access
* **Network Segmentation:** Isolated guest network

✅ **Recommended Enhancements:**

* **Biometric Authentication for Data Centers**
* **Stronger Password Policies**
* **Firewall & Intrusion Prevention Systems**
* **Multi-Factor Authentication for VPNs**

✅ **Final Summary:** 🚀 Successfully completed **Packet Tracer Network Security Exploration Lab!**

* **Applied security best practices (IoT, VPN, WLAN, ACLs)**
* **Validated secure network connectivity**
* **Ensured network segmentation & restricted unauthorized access**

🎯 **This report is ready for GitHub!** 🔥🚀