**Home Network Project Documentation**

**Project Overview**

This project involves setting up an intermediate-level home network using Cisco Packet Tracer. The network includes both wired and wireless devices, IoT devices, and various network services like DHCP, DNS, and NAT. The project focuses on creating a secure and segmented network environment.

**1. Network Topology**

**Diagram:**

A visual representation of the network topology should be created using Cisco Packet Tracer, showing the connections between all devices.

This includes the following:

* Switch connected to PC1, PC2, Printer, and Server.
* Wireless Router connected to the Switch and providing WLAN connectivity to Laptop1, Laptop2, Smartphones, and IoT Devices.

**2. IP Addressing Scheme**

**Network Segments:**

* LAN: 192.168.1.0/24
* PC1: 192.168.1.2
* PC2: 192.168.1.3
* Printer: 192.168.1.10
* WLAN: 192.168.2.0/24
* Laptop1: DHCP (Range: 192.168.2.10 - 192.168.2.100)
* Laptop2: DHCP (Range: 192.168.2.10 - 192.168.2.100)
* Smartphones: DHCP (Range: 192.168.2.10 - 192.168.2.100)
* IoT Network: 192.168.3.0/24
* Smart Light: DHCP (Range: 192.168.3.10 - 192.168.3.50)
* Smart Plug: DHCP (Range: 192.168.3.10 - 192.168.3.50)
* Server Network: 192.168.4.0/24
* Server: 192.168.4.2

**3. Device Configurations**

**3.1. Wireless Router Configuration**

* LAN Interface:
* IP Address: 192.168.1.1/24
* WLAN Interface:
* SSID: HomeWiFi
* Security: WPA2-PSK
* Passphrase: [Your Secure Passphrase]
* IP Address: 192.168.2.1/24
* IoT Network Interface:
* IP Address: 192.168.3.1/24
* Server Network Interface:
* IP Address: 192.168.4.1/24
* DHCP Configuration:
* WLAN DHCP Pool:
* Range: 192.168.2.10 - 192.168.2.100
* Default Gateway: 192.168.2.1
* IoT DHCP Pool:
* Range: 192.168.3.10 - 192.168.3.50
* Default Gateway: 192.168.3.1

**3.2. Switch Configuration**

* Ports:
* Port 1: Connected to PC1
* Port 2: Connected to PC2
* Port 3: Connected to Printer
* Port 4: Connected to Server
* Port 5: Connected to Wireless Router (LAN Interface)

**3.3. Device IP Configurations**

* PC1:
* IP Address: 192.168.1.2/24
* Default Gateway: 192.168.1.1
* PC2:
* IP Address: 192.168.1.3/24
* Default Gateway: 192.168.1.1
* Printer:
* IP Address: 192.168.1.10/24
* Default Gateway: 192.168.1.1
* Server:
* IP Address: 192.168.4.2/24
* Default Gateway: 192.168.4.1

**3.4. Wireless Devices Configuration**

* Laptop1, Laptop2, Smartphones:
* Connect to SSID: HomeWiFi using WPA2-PSK
* Obtain IP Address via DHCP

**3.5. IoT Devices Configuration**

* Smart Light, Smart Plug:
* Connect to IoT Network using appropriate credentials
* Obtain IP Address via DHCP

**4. Security Configurations**

**4.1. Wireless Security**

* SSID: HomeWiFi
* Security: WPA2-PSK
* Passphrase: [Your Secure Passphrase]
* MAC Filtering: Enabled (Add the MAC addresses of trusted devices)

**4.2. IoT Security**

* Access Control Lists (ACLs):
* Deny: IoT devices access to the LAN and WLAN segments.
* Permit: IoT devices to communicate only within the IoT network and to the internet.

**4.3. NAT Configuration**

* NAT:
* Configure NAT on the Wireless Router to allow devices from all network segments (LAN, WLAN, IoT) to access the internet.

**5. Network Services Configuration**

**5.1. DHCP Service**

* WLAN DHCP Pool:
* Range: 192.168.2.10 - 192.168.2.100
* Default Gateway: 192.168.2.1
* DNS Server: 192.168.4.2 (Server)
* IoT Network DHCP Pool:
* Range: 192.168.3.10 - 192.168.3.50
* Default Gateway: 192.168.3.1
* DNS Server: 192.168.4.2 (Server)

**5.2. DNS Service**

* Server Configuration:
* DNS Server: 192.168.4.2
* DNS Records: Add A records for local devices (e.g., pc1.home.local, laptop1.home.local).

**5.3. File Server**

* File Sharing:
* Set up file shares on the Server.
* Allow access to these shares from PCs and Laptops.

**6. Testing and Verification**

**6.1. Connectivity Tests**

* PC1 to PC2:
* Ping 192.168.1.3 (PC2)
* Laptop1 to Laptop2:
* Ping 192.168.2.11 (Laptop2)
* PC1 to Server:
* Ping 192.168.4.2 (Server)
* Smartphone1 to IoT Devices:
* Control Smart Light and Smart Plug

**6.2. Internet Access**

* PC1, Laptop1, Smartphone1:
* Browse to a public website (e.g., www.google.com) to verify internet access.

**6.3. File Sharing**

* PC1:
* Access shared files on the Server via network share (e.g., \\192.168.4.2\shared).
* Laptop1:
* Access shared files on the Server via network share.

**6.4. Security Verification**

* MAC Filtering:
* Attempt to connect an unauthorized device to the WLAN and verify it's blocked.
* ACLs:
* Test that IoT devices cannot access the LAN and WLAN segments.

---

**7. Conclusion**

This documentation covers the step-by-step process of setting up an intermediate home network using Cisco Packet Tracer. The network is segmented into different subnets for better management and security, with proper configurations for IP addressing, DHCP, DNS, and NAT services. The security measures, including WPA2-PSK for wireless and ACLs for IoT devices, ensure that the network is protected from unauthorized access.