



Graduation Project

Wireless Network Deployment Configuration

Cisco Network Administrator

ONL2_ISS4_S1

Made by

Donia Hamdy Awad

Nehal Desouky Ismail

Mariam Moustafa Mahmoud

Yasmine Yahia Elmetwally

Heba allah tarek fathy

Supervised by Eng. Amr Reda

Table of Content

1.Introduction.....	3
2.Document Purpose	3
3.Key Features	4
4.Technical Solution Overview.....	6
5.Introduction to Wireless.....	8
6.Solution Components.....	14
7.Network Architecture	16
7.1.WPA2 Enterprise using Radius Server in WLC on Home Router.....	17
7.2.WPA2 Enterprise using Radius Server in WLC.....	20
7.3.WLC WPA2 Personal.....	24
7.4.Home router.....	31
7.55. IOT (Internet of things).....	35

1. Introduction

This document provides a detailed explanation of each section in the network topology, along with a brief on AAA (Authentication, Authorization, and Accounting) used in the design.:

This network topology shows a complete and realistic wireless setup that includes different types of environments: a smart home with IoT devices, simple wireless connections using WPA2 Personal, and advanced enterprise-level networks using WPA2 Enterprise and Wireless LAN Controllers (WLCs).

The smart home area has connected devices like lights, fans, door locks, and sensors, all controlled through a home gateway. Other parts of the topology use wireless routers and access points to connect laptops, smartphones, and tablets securely.

Some areas use Radius servers and the AAA system (Authentication, Authorization, and Accounting) to control who can access the network and what they can do. This helps keep the network safe and organized, especially in bigger or more sensitive environments.

2.Document Purpose

Design the wireless network including access point placement, SSIDs, and security settings, Test wireless coverage and performance. Optimize channel settings and address any connectivity issues

The purpose of this topology is to demonstrate how different wireless technologies and security methods can be combined in one network. It shows how a smart home can be connected with IoT devices, how personal wireless networks work using WPA2 Personal, and how enterprise networks use WPA2 Enterprise with centralized control through WLCs.

It also highlights the importance of using AAA (Authentication, Authorization, and Accounting) for secure user management, especially in professional environments. This setup can be used for learning, testing, or simulating real-world wireless network scenarios.

3. Key Features

1. Wireless LAN Controller (WLC) Configuration

- a. Setup and management of centralized wireless networks using WLC.
- b. Enhanced wireless performance and control.

2. Client Roaming Support

- a. Configuration to allow seamless roaming between access points.
- b. Ensures uninterrupted connectivity for mobile devices.

3. Enterprise-Level Security with RADIUS Server

- a. Implementation of 802.1x authentication.
- b. Integration of a RADIUS server for secure user management.
- c. Use of a shared key for encrypted communication.

4. Laptop Profile Configuration

- a. Manual creation of wireless profiles on end-user devices.
- b. Testing and verification of client connectivity to enterprise networks.

5. VLAN Segmentation in WLC

- a. Creation and assignment of VLANs to separate network traffic.
- b. Setup of DHCP pools for dynamic IP addressing within VLANs.

6. End-to-End Connectivity Verification

- a. Comprehensive testing of wireless configurations and network access.
- b. Troubleshooting and validation steps for successful deployment.

7. IoT Integration in Packet Tracer

- a. Simulated deployment of Internet of Things (IoT) devices.
- b. Practical implementation of motion detection with remote server interaction.

4. Technical Solution Overview

This project presents a comprehensive wireless networking solution using Cisco Packet Tracer, focusing on the simulation and configuration of enterprise-grade wireless infrastructure. The architecture integrates IoT devices, Wireless LAN Controllers (WLC), RADIUS-based authentication.

1. Internet of Things (IoT) Integration

- Deployed IoT devices such as motion detectors.
- Configured remote server interactions to enable real-time response.
- Demonstrated the use of IoT within a secure wireless environment.

2. Wireless LAN Controller (WLC) Setup

- Configured WLC to manage multiple Access Points (APs).
- Centralized wireless policy and SSID deployment.
- Enabled and verified seamless roaming capabilities between APs.

3. Enterprise Security with RADIUS Server

- Implemented RADIUS server for secure 802.1x-based authentication.
- Configured shared keys to ensure encrypted communication.

- Created user profiles for controlled network access.

4. Client-Side Configuration

- Wireless profiles were configured on laptops to connect securely to the WLAN.
- Verified successful authentication and data transmission through RADIUS.

5. VLAN Configuration and DHCP Integration

- Assigned DHCP pools to each VLAN for dynamic IP addressing.

6. Testing and Validation

- Verified end-to-end connectivity between clients, APs, WLC, and remote servers.
- Conducted roaming tests and IoT event simulation (motion detection).
- Ensured proper communication flow across all layers of the simulated architecture.

From this we can talk about Wireless and the different things in our project

5. Introduction to Wireless

Benefits of Wireless

- A Wireless LAN (WLAN) is a type of wireless network that is commonly used in homes, offices, and campus environments.
- WLANs make mobility possible within the home and business environments.
- Wireless infrastructures adapt to rapidly changing needs and technologies.

Types of Wireless Networks

- Wireless Personal-Area Network (WPAN) - Low power and short-range (20-30ft or 6-9 meters). Based on IEEE 802.15 standard and 2.4 GHz frequency. Bluetooth and Zigbee are WPAN examples.
- Wireless LAN (WLAN) - Medium sized networks up to about 300 feet. Based on IEEE 802.11 standard and 2.4 or 5.0 GHz frequency.
- Wireless MAN (WMAN) - Large geographic area such as city or district. Uses specific licensed frequencies.
- Wireless WAN (WWAN) - Extensive geographic area for national or global communication. Uses specific licensed freq

WLAN Components

Wireless Home Router

- A home user typically interconnects wireless devices using a small, wireless router.
- Wireless routers serve as the following:
 - Access point - To provide wires access
 - Switch - To interconnect wired devices

- Router - To provide a default gateway to other networks and the Internet

Wireless Access Point

Wireless clients use their wireless NIC to discover nearby access points (APs).

Clients then attempt to associate and authenticate with an AP.

After being authenticated, wireless users have access to network resources.



AP Categories

APs can be categorized as either autonomous APs or controller-based APs.

- Autonomous APs - Standalone devices configured through a command line interface or GUI. Each autonomous AP acts independently of the others and is configured and managed manually by an administrator.
- Controller-based APs - Also known as lightweight APs (LAPs). Use Lightweight Access Point Protocol (LWAPP) to communicate with a LWAN controller (WLC). Each LAP is automatically configured and managed by the WLC

WLAN Operation

Wireless Client and AP Association

For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

Wireless devices complete the following three stage process:

- Discover a wireless AP
- Authenticate with the AP
- Associate with the AP

To achieve successful association, a wireless client and an AP must agree on specific parameters:

- SSID-The client needs to know the name of the network to connect.
- Password - This is required for the client to authenticate to the AP.
- Network mode - The 802.11 standard in use.
- Security mode - The security parameter settings, i.e. WEP, WPA, or WPA2.
- Channel settings - The frequency bands in use.

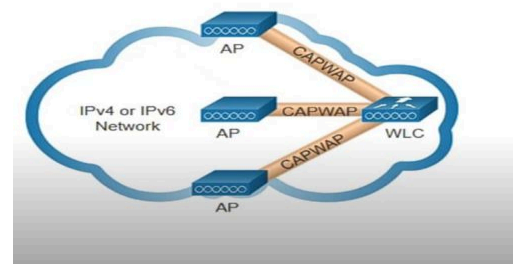
CAPWAP Operation

Introduction to CAPWAP

CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANS. Based on LWAPP but adds additional security with Datagram Transport Layer Security (DTLS).

Encapsulates and forwards WLAN client traffic between an AP and a WLC over tunnels using UDP ports 5246 and 5247.

Operates over both IPv4 and IPv6. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.

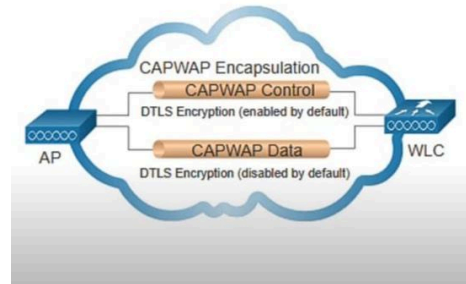


DTLS Encryption

DTLS provides security between the AP and the WLC.

It is enabled by default to secure the CAPWAP control channel and encrypt all management and control traffic between AP and WLC.

Data encryption is disabled by default and requires a DTLS license to be installed on the WLC before it can be enabled on the AP.



Secure WLANS

SSID Cloaking and MAC Address Filtering

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs:

SSID Cloaking : APs and some wireless routers allow the SSID beacon frame to be disabled. Wireless clients must be manually configured with the SSID to connect to the network.

MAC Address Filtering : An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. In the figure, the router is configured to permit two MAC addresses. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.

802.11 Original Authentication Methods

The best way to secure a wireless network is to use authentication and encryption systems. Two types of authentication were introduced with the original 802.11 standard:

Open system authentication

-No password required. Typically used to provide free internet access in public areas like cafes, airports, and hotels.

-Client is responsible for providing security such as through a VPN.

Shared key authentication

Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2, with WPA 2 having two authentication methods.

Personal Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.

Enterprise - Intended for enterprise networks. Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

Encryption Methods

Advanced Encryption Standard (AES)

- Used by WPA2 and uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and unencrypted bits have been altered.

Authentication in the Enterprise

Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

There pieces of information are required:

RADIUS server IP address - IP address of the server.

UDP port numbers -UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646.

Shared key - Used to authenticate the AP with the RADIUS server

6.Solution Components

1. Cisco Packet Tracer

- Simulation environment for designing and testing network topologies.
- Provides virtual access points, controllers, servers, and IoT devices.

2. Wireless LAN Controller (WLC)

- Centralized device for managing access points and wireless policies.
- Handles SSID broadcasting, security configurations.

3. Access Points (APs)

- Wireless devices that extend network connectivity to mobile and IoT devices.
- Configured and managed through WLC.
- Enable seamless roaming for clients.

4. RADIUS Server

- Authenticates users via 802.1x protocol.
- Stores user credentials and enforces access control.
- Uses a shared secret for secure communication with the WLC.

5. IoT Devices

- Simulated smart devices (e.g., motion sensors).
- Connected via wireless network to interact with a remote server.
- Serve as part of the smart automation demo.

6. Remote Server

- Processes data from IoT devices (e.g., triggers from motion detection).
- Acts as a backend for IoT communication.

7. Laptops / End Devices

- Simulate user endpoints requiring wireless connectivity.
- Configured with custom wireless profiles to access enterprise WLANs.
- Used to test roaming, authentication, and connectivity.

8. VLANs and DHCP Server

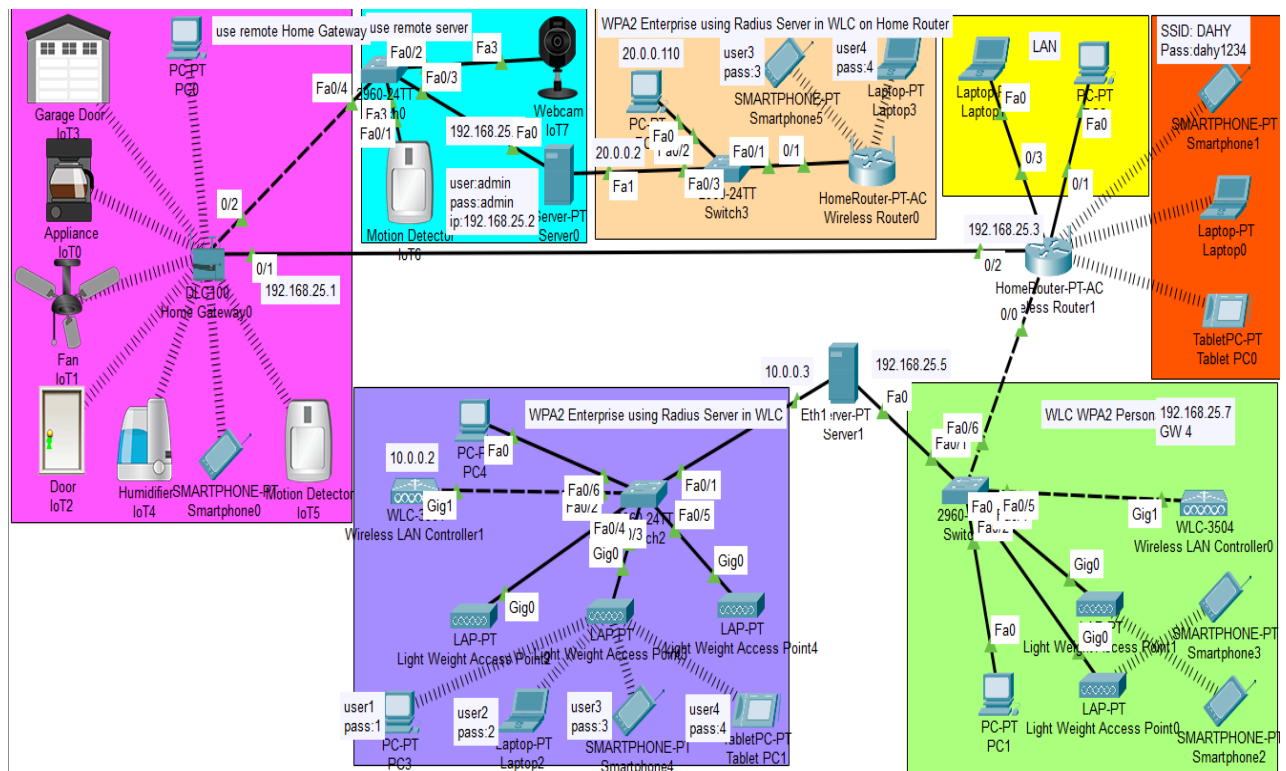
- VLANs separate traffic by function or user group.
- DHCP server assigns IP addresses dynamically within each VLAN.

9. Network Switches

- Facilitate wired connections between WLC, RADIUS server, and DHCP server.
- Enable trunking and VLAN propagation across the infrastructure.

6.Network Architecture

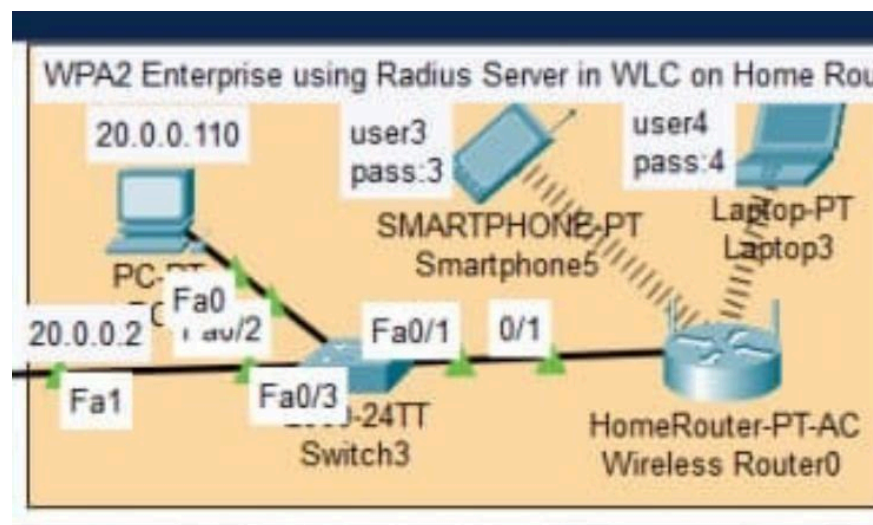
Physical Topology



This Network topology has three LANs

1. WPA2 Enterprise using Radius Server in WLC
2. WPA2 Enterprise using Radius Server in WLC on Home Router
3. WLC WPA2 Personal, Home router and IOT

1.WPA2 Enterprise using Radius Server in WLC on Home Router



1. Introduction

This document explains the configuration and function of a WPA2 Enterprise wireless network using a HomeRouter-PT-AC router and a Radius server embedded in a Wireless LAN Controller (WLC). It is designed for secure wireless access where each user logs in with a unique username and password.

2. Network Components

- HomeRouter-PT-AC: The main wireless router broadcasting WPA2 Enterprise SSID.
- Switch3: Connects router, WLC, and devices.
- WLC-1 (Wireless LAN Controller): Contains the internal Radius server responsible for authentication.
- Devices: Laptop3 and Smartphone4 connect using their credentials.

3. Authentication Process

1. The user attempts to connect to the Wi-Fi network.
2. They enter a specific username and password (e.g., user3/pass:3).
3. The router forwards these credentials to the Radius server inside the WLC.
4. The Radius server checks the validity of the credentials:
 - If correct: access is granted.
 - If incorrect: access is denied.
5. If access is denied, the device shows a failure message and is not connected to the network.

4. Role of the Controller (WLC)

The WLC serves a dual purpose in this setup:

- Acts as the internal Radius Server that authenticates users.
- Manages Wi-Fi access policies, logs authentication attempts, and ensures secure user validation.

5. WPA2 Personal vs WPA2 Enterprise

Comparison between traditional WPA2 Personal and WPA2 Enterprise:

WPA2 Personal:

- Shared password for all users.
- Moderate security.
- No individual control.

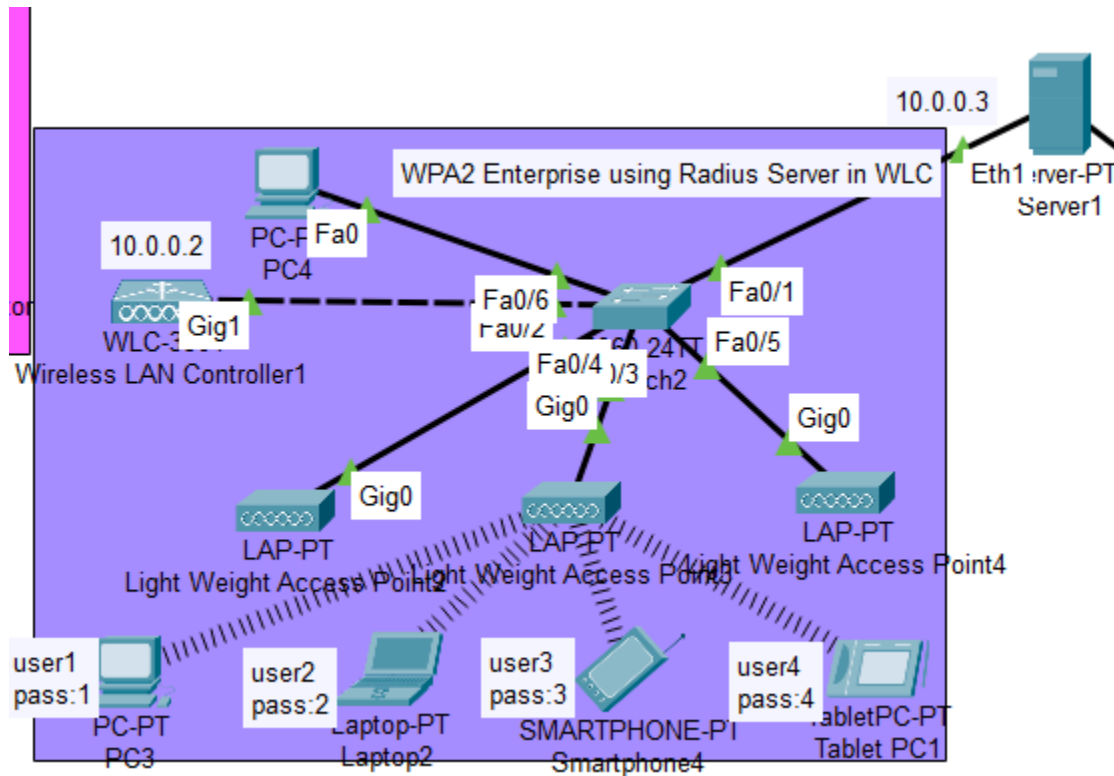
WPA2 Enterprise:

- Each user has a unique username and password.
- High security and central control.
- Requires Radius Server (managed by WLC in this case).

6. Conclusion

WPA2 Enterprise networks, especially with the help of a Radius Server embedded in a Wireless LAN Controller, provide a higher level of security and user management. Each device must authenticate individually, which prevents unauthorized access and allows for detailed monitoring and control.

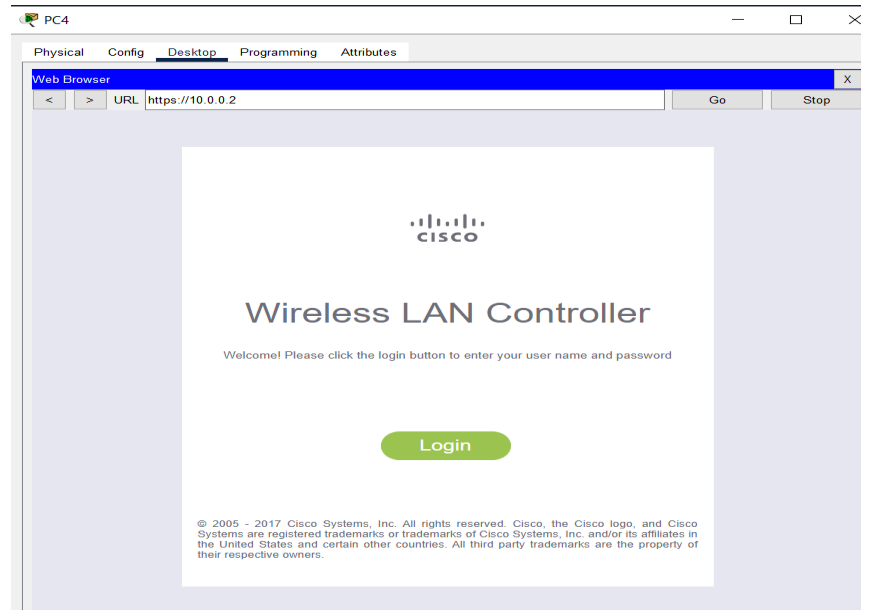
2.WPA2 Enterprise using Radius Server in WLC



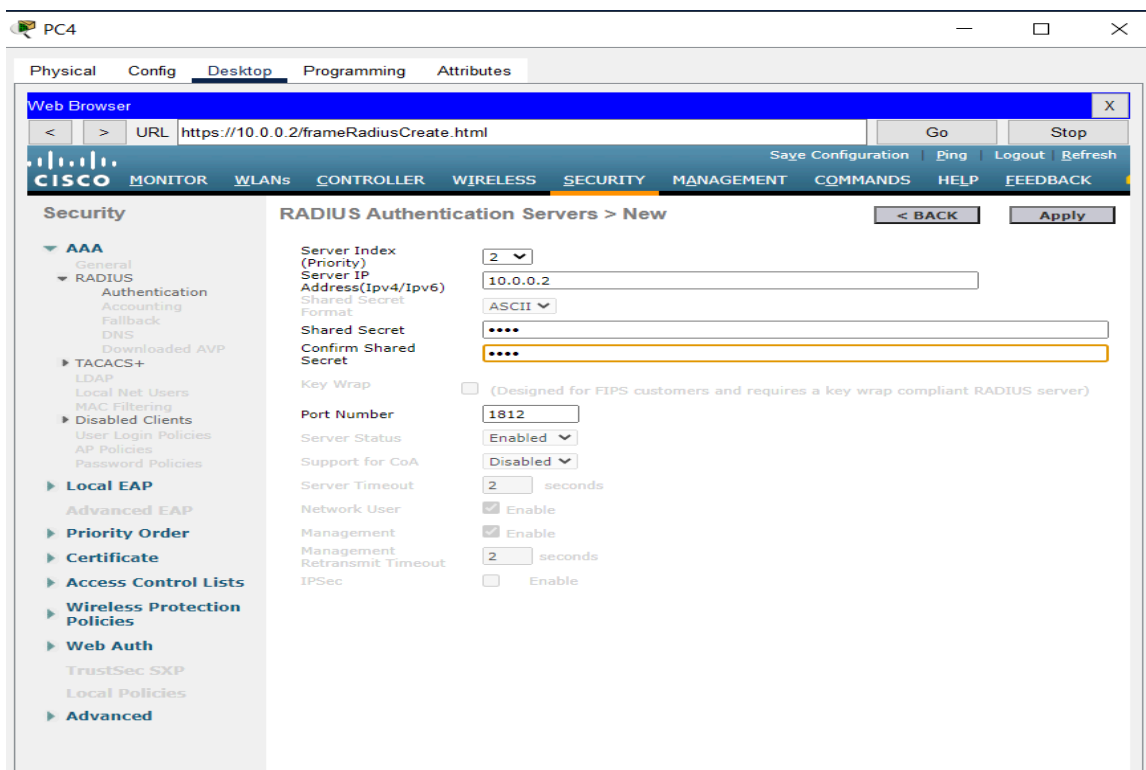
WPA2-Enterprise using a RADIUS server in WLC on a home router refers to a network setup where:

- **WPA2-Enterprise** is a Wi-Fi security protocol that uses individual credentials for each user instead of a shared password.
- **RADIUS server** (Remote Authentication Dial-In User Service) is used to authenticate users centrally. It checks user credentials and grants access.
- **WLC** (Wireless LAN Controller) manages wireless access points and enforces network policies.

Entering the WLC:

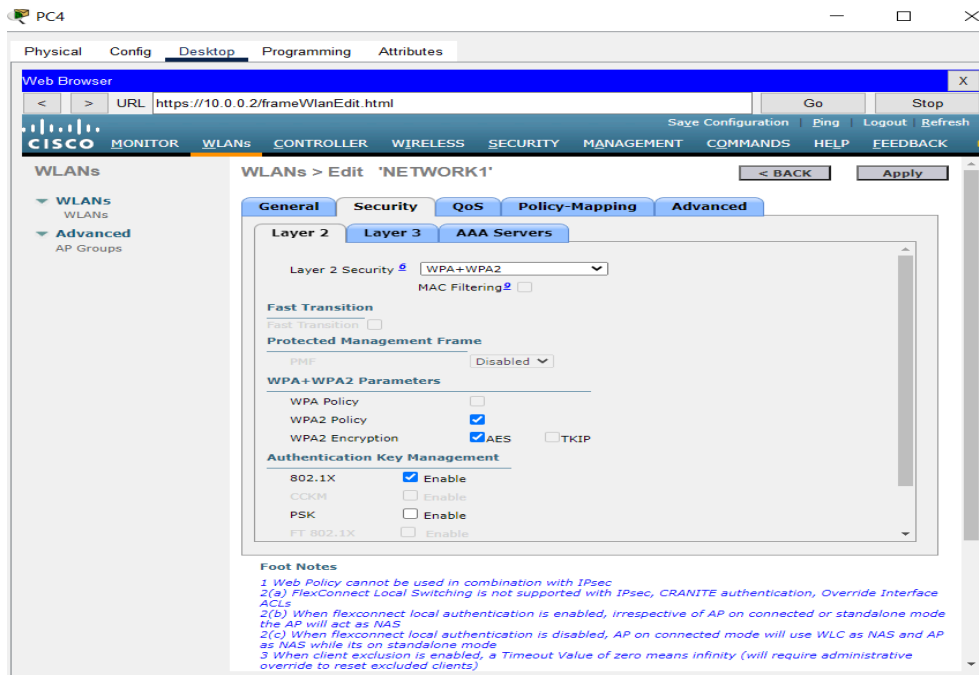


Configuring Radius server:

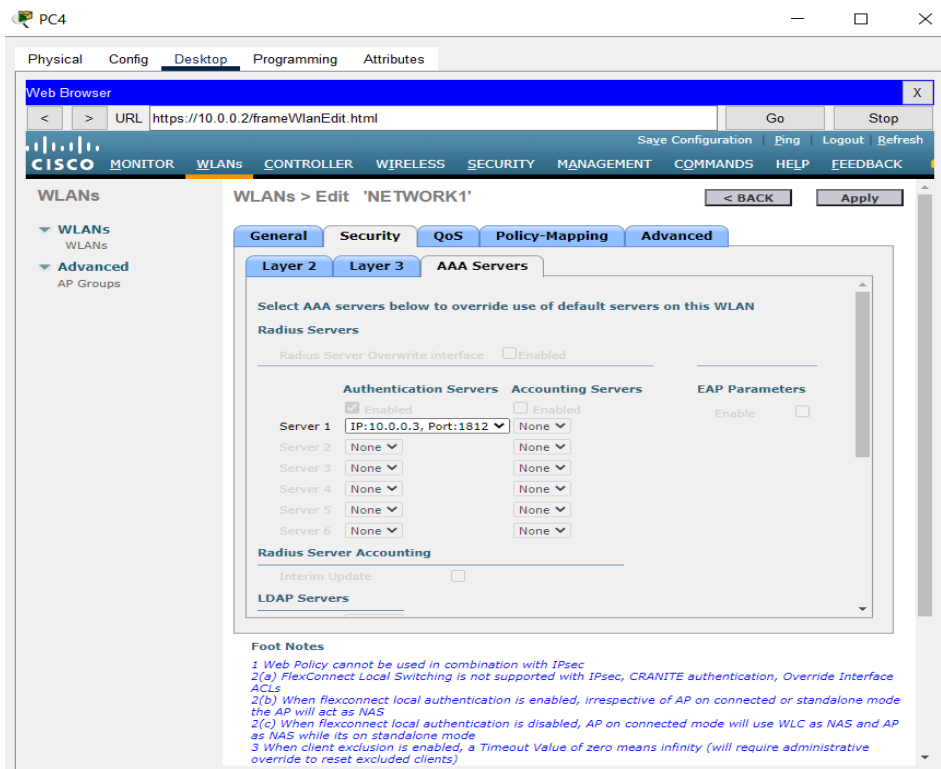


Security:

- WPA2-Enterprise on Layer 2:



- AAA on WLC



- AAA on Server

The screenshot shows the 'Server1' configuration window with the 'Services' tab selected. The 'AAA' service is configured with the following settings:

- Service:** On (radio button selected), Off (radio button unselected)
- Radius Port:** 1812
- Network Configuration:**
 - Client Name:** NETWORK1
 - Client IP:** 10.0.0.2
 - Secret:** dahy
 - ServerType:** Radius
- User Setup:**

	Username	Password
1	user1	1
2	user2	2
3	user3	3
4	user4	4

Adding the network on a smart-phone:

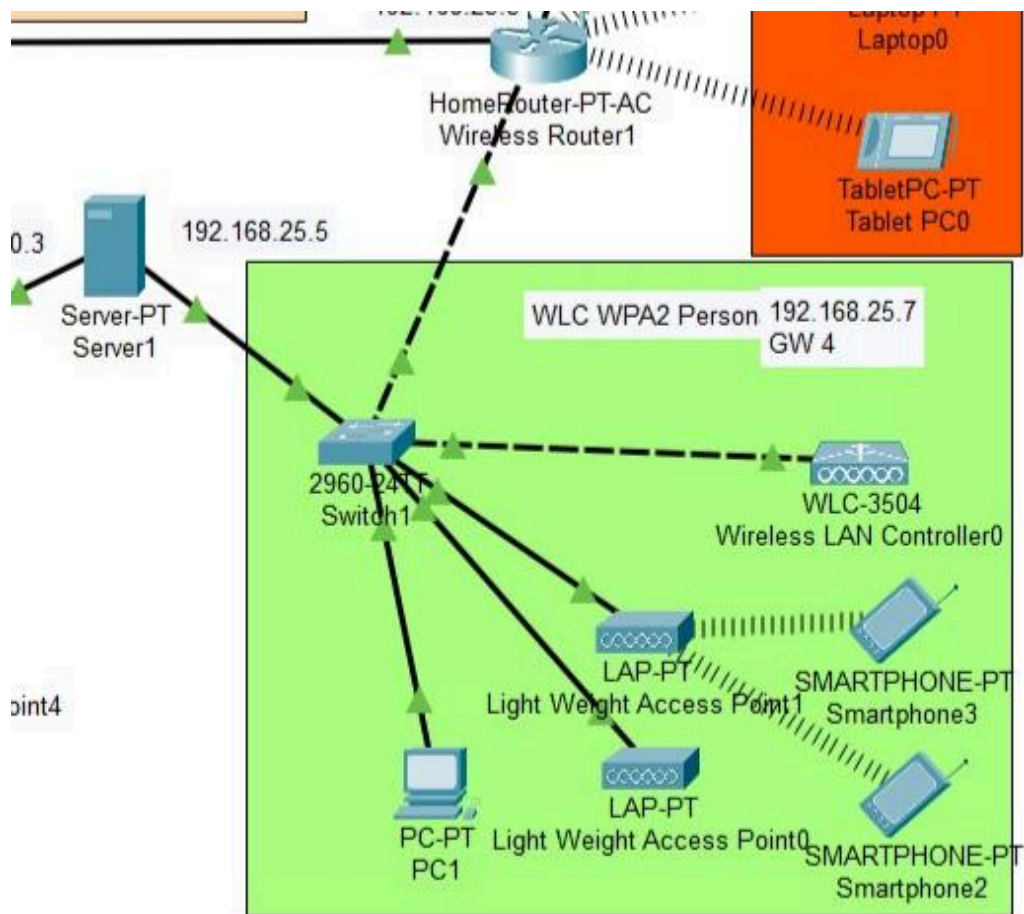
The screenshot shows the 'Smartphone4' configuration window with the 'Config' tab selected. The 'Wireless0' interface is configured with the following settings:

- Port Status:** On (checkbox checked)
- Bandwidth:** 300 Mbps
- MAC Address:** 00D0.BC39.8EE8
- SSID:** NETWORK1
- Authentication:**
 - ☐ Disabled
 - ☐ WPA-PSK
 - ☐ WPA
 - ☐ 802.1X
 - ☐ WEP
 - ☐ WPA2-PSK
 - ☒ WPA2
- Method:** MD5
- Encryption Type:** AES
- IP Configuration:**
 - ☒ DHCP
 - ☐ Static
 - IPv4 Address:** 10.0.0.17
 - Subnet Mask:** 255.0.0.0
- IPv6 Configuration:**
 - ☒ Automatic
 - ☐ Static
 - IPv6 Address:** FE80::2D0:BCFF:FE39:8EE8
 - Link Local Address:** FE80::2D0:BCFF:FE39:8EE8

3.WLC WPA2 Personal

Personal - Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.

this network get Dhcp ip from home gateway 192.168.25.1, The RADIUS server is the DHCP server for the WLC WPA2 Personal



- **For WLC configuration**

From RADIUS server that we put "sever 1" we will use DHCP and activated for the network

the pool name is serverPool , This pool is the distributor of the IP address for the 192.168.25.1 network to the devices there.

The screenshot shows the 'Services' tab in the Cisco WLC configuration interface. The 'DHCP' service is selected in the left-hand 'SERVICES' list. The configuration for the DHCP service is shown on the right, with the following details:

- Interface:** FastEthernet0
- Service:** On (radio button selected)
- Pool Name:** serverPool
- Default Gateway:** 192.168.25.1
- DNS Server:** 0.0.0.0
- Start IP Address:** 192.168.25.30
- Subnet Mask:** 255.255.255.0
- Maximum Number of Users:** 10
- TFTP Server:** 0.0.0.0
- WLC Address:** 192.168.25.7

Below the configuration fields, there are 'Add', 'Save', and 'Remove' buttons. A table at the bottom lists the configured DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.25.1	0.0.0.0	192.168.25.30	255.255.255.0	10	0.0.0.0	192.168.25.7

this is Ip of Pc1

The screenshot shows the 'IP Configuration' window for PC1. The 'Interface' is set to 'FastEthernet0'. The 'IP Configuration' section is expanded, showing the following details:

- IP Configuration:** DHCP (radio button selected)
- IPv4 Address:** 192.168.25.33
- Subnet Mask:** 255.255.255.0
- Default Gateway:** 192.168.25.1
- DNS Server:** 0.0.0.0

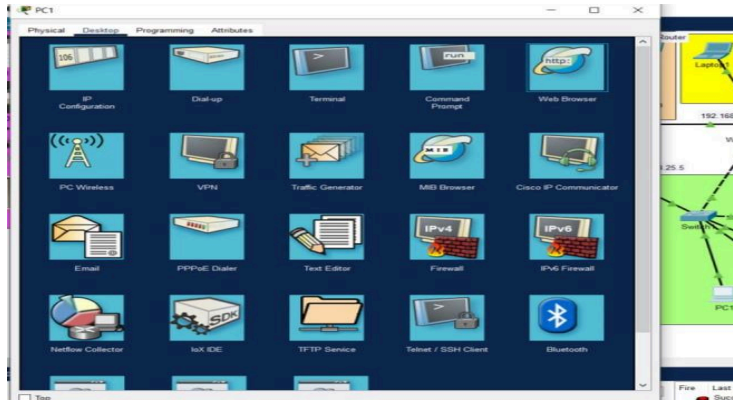
The 'IPv6 Configuration' section is also visible, with the following details:

- IPv6 Configuration:** Static (radio button selected)
- IPv6 Address:** FE80:210:11FF:FE98:DE2A
- Link Local Address:** FE80:210:11FF:FE98:DE2A
- Default Gateway:**
- DNS Server:**

At the bottom, there are checkboxes for '802.1X' and 'Use 802.1X Security', and fields for 'Authentication', 'Username', and 'Password'.

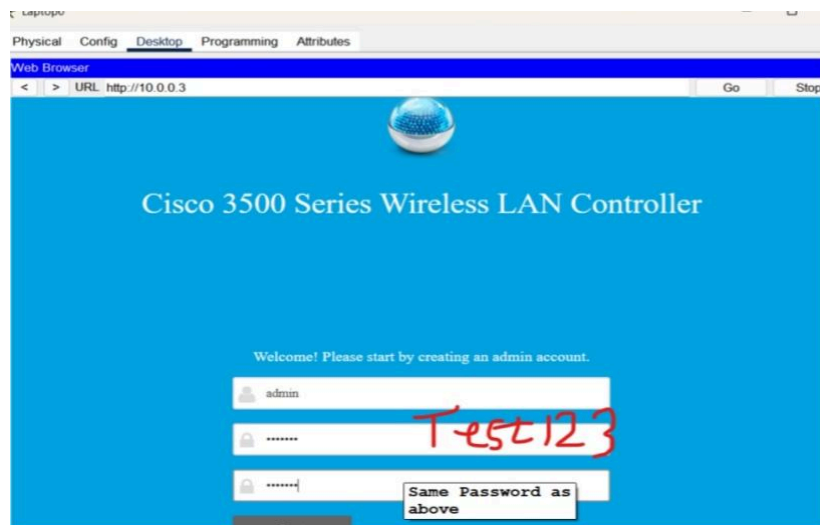
then from pc 1 we will make the configuration of WLC

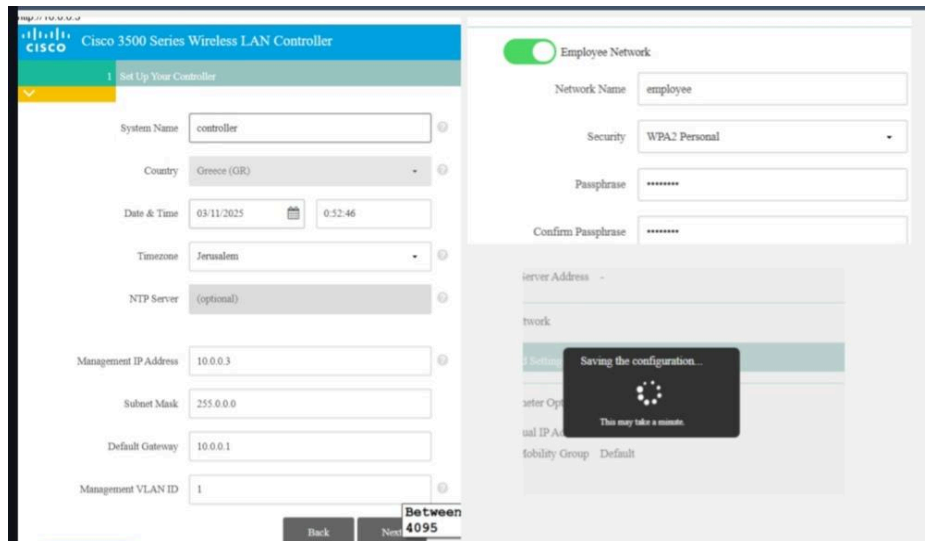
- CLICK on pc1
- click on Web browser
- enter ip of Wlc 192.168.25.7



This screen will appear to us. so have to sign up

- use name admin
- password Test123 and we have to confirm it again





then by ip we connected to the page of wlc

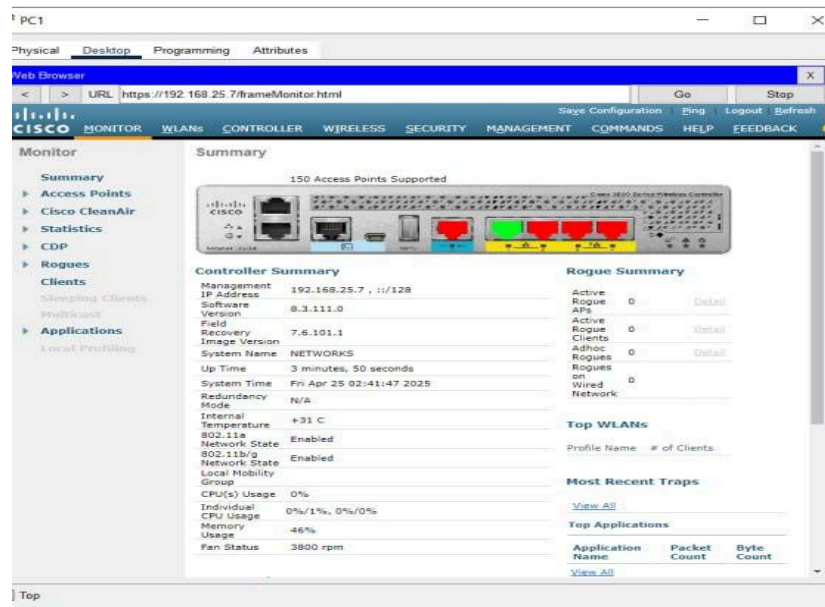


username: admin

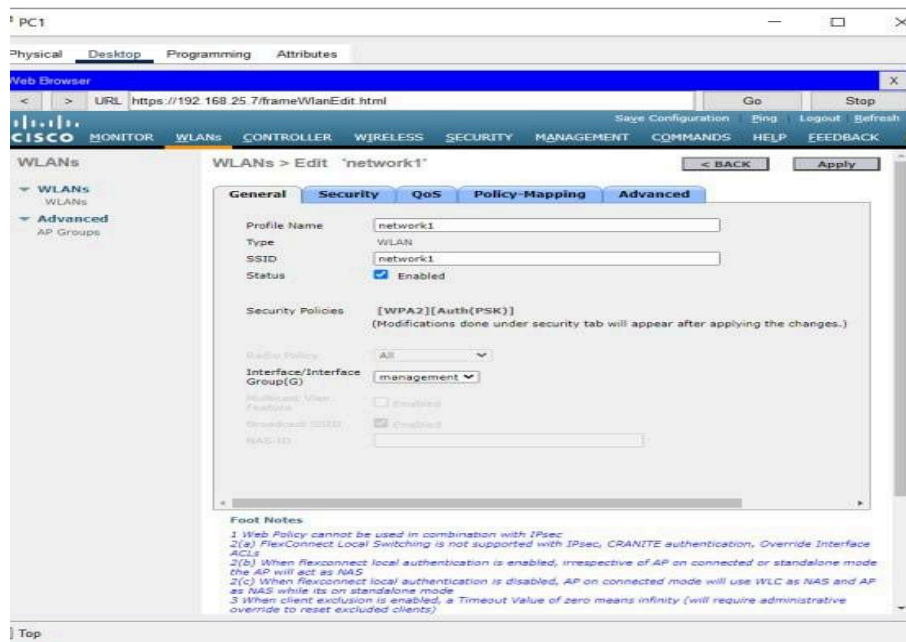
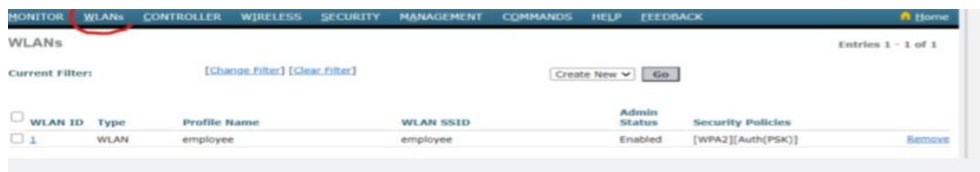
password : admin

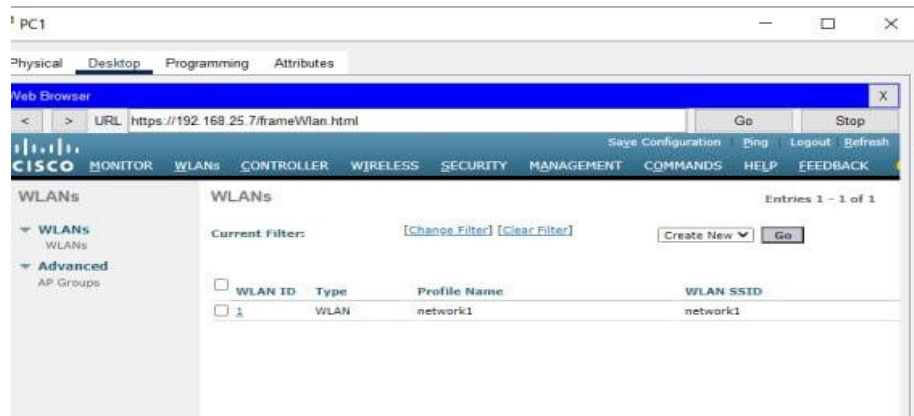


this is the WLC from inside



then from WLAN we can create a Network with name “ssid” the name of the network here is “ network 1”.





and we have here two Ap so we have to apply Roaming too

"Roaming" in the context of wireless networks refers to the ability of a device to move seamlessly between different Access Points (APs) within the same network without losing connection. As a device moves from one AP's coverage area to another, the network ensures that the device maintains its connection by switching to the nearest or strongest AP.

Regarding WPA2 Personal on WLC (Wireless LAN Controller): Yes, roaming can be applied in WPA2 Personal networks, but with some limitations. WPA2 Personal uses a pre-shared key (PSK) for authentication, which may require some additional handling in a roaming scenario. The roaming process itself typically works more smoothly in enterprise environments (using WPA2 Enterprise and 802.1X authentication), where the transition between APs is managed more dynamically. However, WPA2 Personal can still support roaming, although it may not be as efficient in some cases as WPA2 Enterprise when it comes to handoff times and security management.

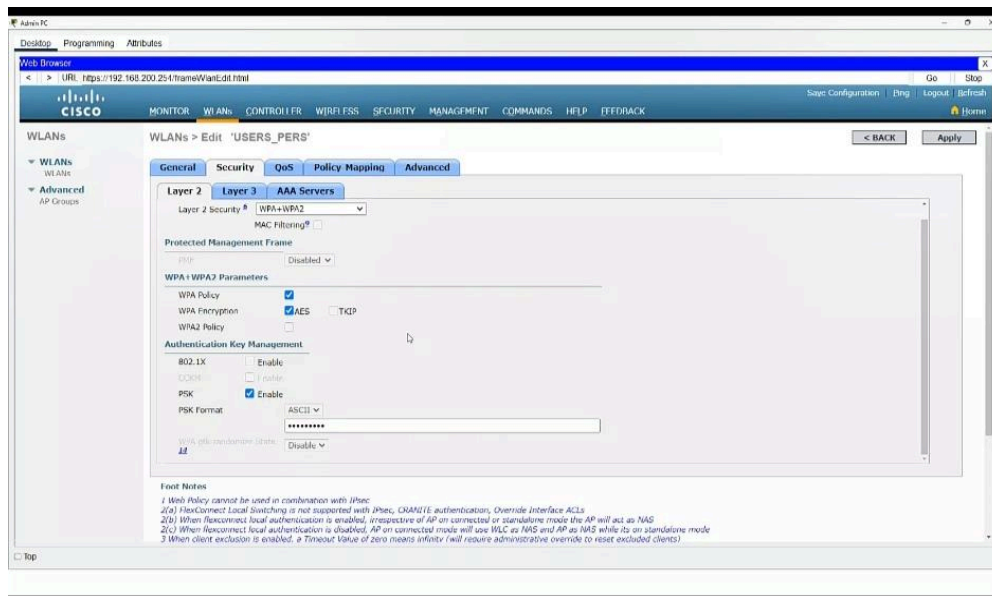
Features like 802.11k and 802.11r can be enabled on a WLC to optimize roaming, even with WPA2 Personal, though the security setup might not be as seamless as in enterprise configurations.

- For security

Layer 2

Security in WPA2 Personal WLAN:

In the WPA2 Personal configuration, the network uses a Pre-Shared Key (PSK) for authentication. This means that all users connect using the same password, which is manually configured on the Wireless LAN Controller (WLC). The data transmitted over the network is encrypted using AES, ensuring confidentiality and protection against eavesdropping. This method is simple to deploy and suitable for small to medium networks that do not require user-specific authentication.



- For VLAN

Here we created a one for WLC WPA2 Personal and it's name is management

- from controller > interfaces > new >
- write a name for it “management” and id it can any number then Apply
- then we have to give it a ip, subnet mask, gateway and port number



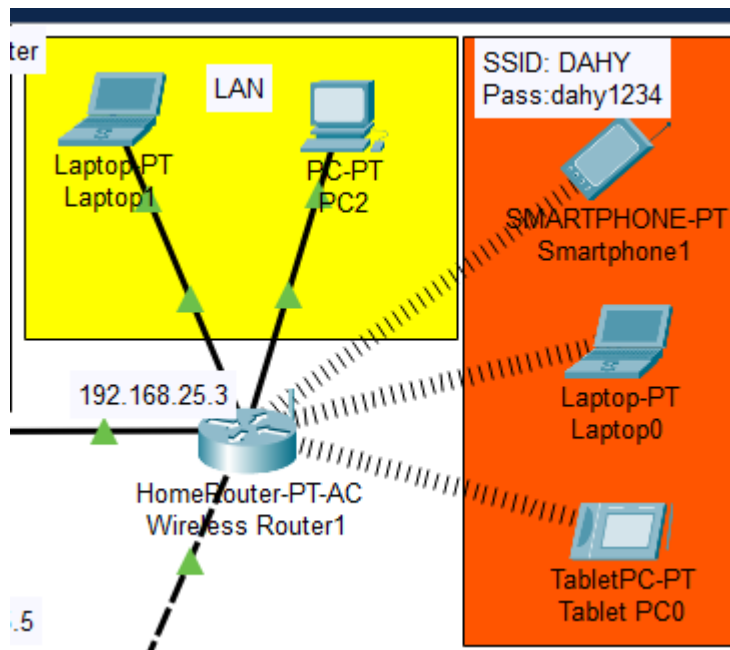
Then we can check the conductivity

4.Home router

In this part of the project, we focus on a central device called **HomeRouter-PT-AC**, which plays a dual role by providing access to both **wireless (Wi-Fi)** and **wired (LAN)** networks for multiple end devices.

Router IP Address: 192.168.25.3

This is the local IP address used by devices to communicate with the router.



Wired Network (LAN)

This part of the network includes devices connected to the router through Ethernet cables (LAN). Wired networks offer higher stability and speed, especially for stationary or high-performance devices.

Connected Devices:

- Laptop1 (*Laptop-PT*)
- PC2 (*PC-PT*)

These devices are connected directly to **HomeRouter-PT-AC** via Ethernet ports, forming the wired segment of the home network.

Wireless Network (SSID: DAHY)

This segment represents the wireless part of the home network. The router broadcasts a Wi-Fi network with the following details:

- **Network Name (SSID):** DAHY
- **Password:** dahy1234
- **Connection Type:** Wireless (Wi-Fi)

Connected Devices:

- Smartphone1 (*SMARTPHONE-PT*)
- Laptop0 (*Laptop-PT*)
- TabletPC0 (*TabletPC-PT*)

All of these devices connect to the HomeRouter-PT-AC via Wi-Fi. They belong to the same wireless network and can access internal network services or external resources through the router.

the Basic Setup page of the **HomeRouter-PT-AC**. The router is configured to obtain its IP automatically via DHCP, and its internal address is set to **192.168.25.3**. The DHCP server is disabled, so connected devices must use static IPs or receive their IP addresses from another DHCP server on the network.

Wireless Router1

Physical Config **GUI** Attributes

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 25 . 3

Subnet Mask: 255.255.255.0

DHCP Server: ☐ Enabled ☒ Disabled

DHCP Reservation

Start IP Address: 192.168.1.100

Maximum number of Users: 50

IP Address Range: 192.168.1.100 - 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

ISP Vlan

☐ Enabled ☒ Disabled

Vlan IDs:

Internet: 10 VoIP: 20 IPTV: 30

Port Vlan:

Port 1: Internet Port 2: Internet Port 3: Internet Port 4: Internet

2.4GHz: Internet 5GHz - 1: Internet 5GHz - 2: Internet

Wireless Security

2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: dahy1234

Wireless Network Monitor showing available Wi-Fi networks. The network 'DAHY' is selected, showing strong signal strength and WPA2-PSK security. This validates that the HomeRouter-PT-AC is correctly broadcasting the wireless network.

→

Link Information

Connect

Profiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
network2	1	43%
HomeGateway	1	31%
DAHY	1	72%

Wireless Mode

Infrastructure

Network Type

Mixed B/G/N

Radio Band

Auto

Security

WPA2-PSK

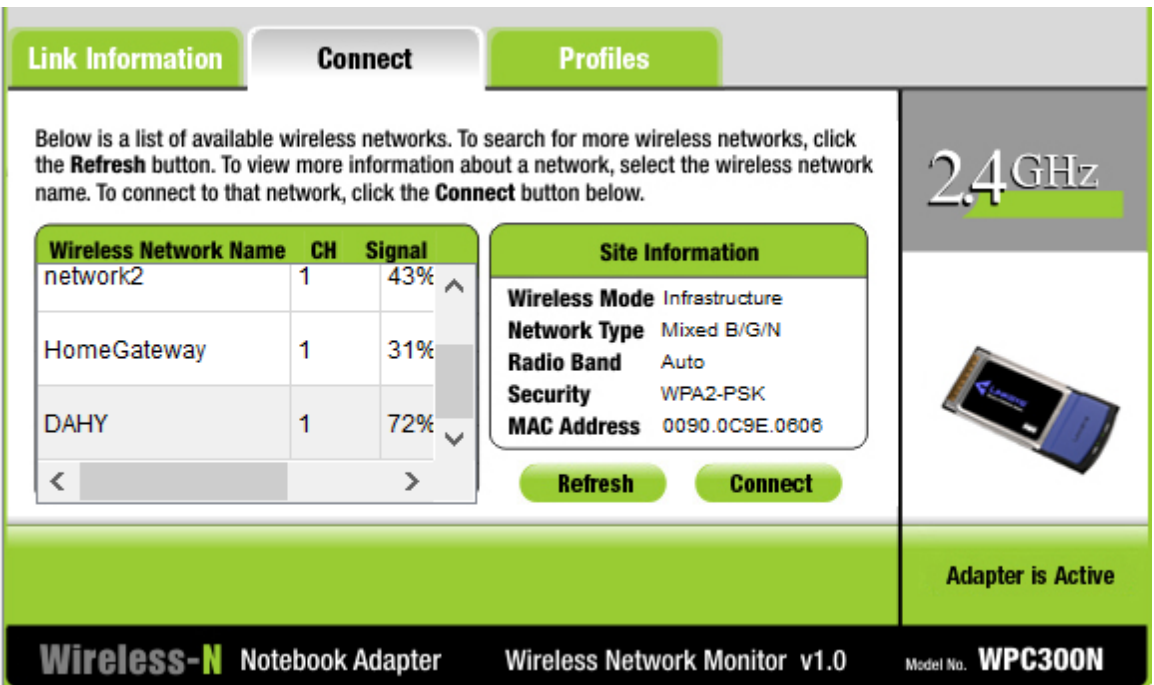
MAC Address

0090.0C9E.0806

Refresh

Connect

2.4GHz



Adapter is Active

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

Link Information

Connect


Profiles

More Information

Infrastructure Mode

You have successfully connected to the access point



Signal Strength 

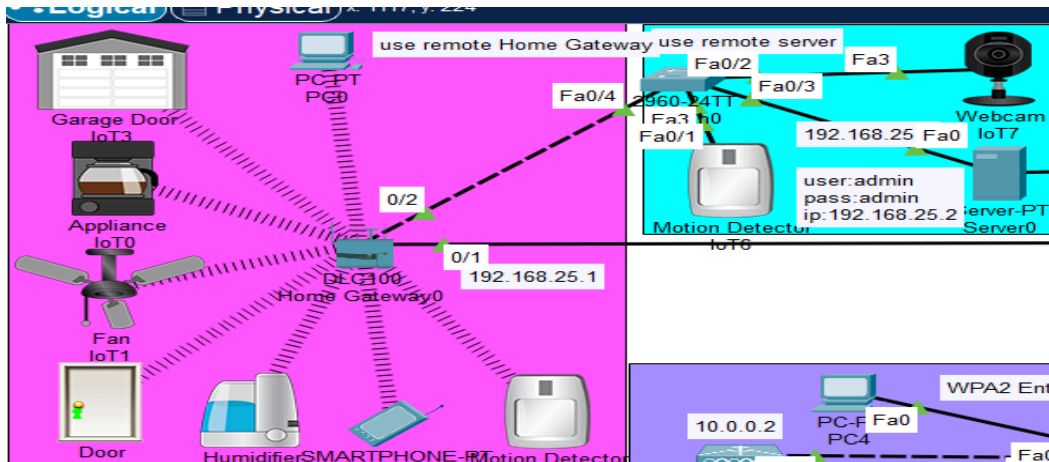
Link Quality 

Adapter is Active

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

5. IOT (Internet of things)

The IoT (Internet of Things) section simulates a smart home environment. It includes various smart devices connected to a central **Home Gateway0**, allowing control and monitoring over a network.



2. IoT Components

(Door,Appliance,Fan,Humidifier,Motion Sensor (Left),Motion Sensor (Right),Smartphone,Home Gateway,Management PC)

3. Network Connectivity

- **Home Gateway0** is the main hub for all IoT devices.
- It connects to:
 - All IoT devices locally (via internal protocols).
 - The network switch (**2960-24TT Switch2**) on port **FastEthernet 0/1**.
 - Its IP address is **192.168.25.1**.

- **Server0** (in the blue area) acts as a **Remote IoT Server** with:
 - Username: **admin**
 - Password: **admin**
 - IP: **192.168.25.2**
 - Used for **remote access** to the IoT system.
- **PC0** is directly connected and used for **local configuration** of Home Gateway0.

5. Use Cases

- Smart home automation (e.g., turn on the fan if the room is hot).
- Remote door control and security monitoring.
- Energy-saving routines and environmental control (humidity, lights, etc.).

6. Additional Notes

- The smartphone (Smartphone0) simulates mobile app control.
- The setup can be extended with:
 - Smart lights
 - Security cameras
 - Fire/smoke detectors
 - Environmental sensors

