VxLEARN Networks

Networking & Cybersecurity Track
Simulated Employment Program

Lab Report:
Configure Basic Wireless Security (WPA2 Personal) Lab

Prepared by:
Kudzaishe Majeza
Junior Network Engineer – VxLEARN Networks

Mentor:
Titus Majeza
Senior Network Engineer

Date: 26 January 2026

Table of Contents

1. Introduction 3
2. Objectives 3
3. Network Topology Overview 3
4. Part 1 – Verify Connectivity (Before Security) 4
5. Part 2 – Configure WPA2 Personal on the Wireless Router 5
6. Part 3 – Update Laptop Wireless Settings 7
7. Part 4 – Verify Connectivity (After Security) 9
8. Security Explanation 9
9. Reflection 9

1. Introduction

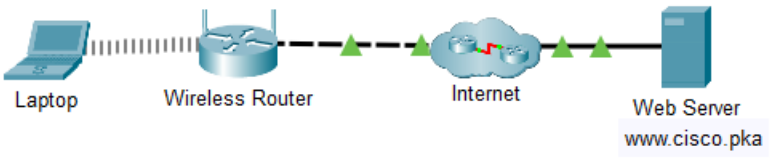
This lab demonstrates how to configure basic wireless security on a small business network using WPA2 Personal. The purpose of the lab is to show how an unsecured wireless network can be protected from unauthorized access while still allowing legitimate users to connect and access network resources.

2. Objectives

- Verify wireless connectivity before security is applied
- Configure WPA2 Personal security on a wireless router
- Reconnect a wireless client using a pre-shared key
- Verify connectivity after security configuration

3. Network Topology Overview

The network consists of a wireless router and a laptop client. Initially, the wireless network is open with no security enabled, allowing any device within range to connect.



Initial network topology

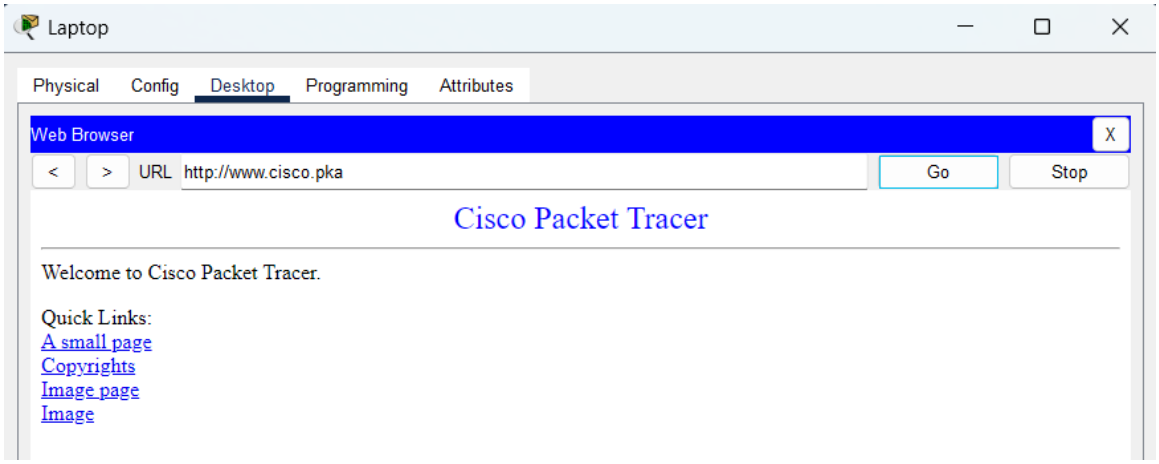
4. Part 1 – Verify Connectivity (Before Security)

Before configuring wireless security, connectivity was tested to confirm that the laptop could successfully access network resources.

Steps performed:

1. Opened the Laptop Desktop tab

2. Accessed the Web Browser
3. Entered www.cisco.pka in the URL field
4. Confirmed the webpage loaded successfully



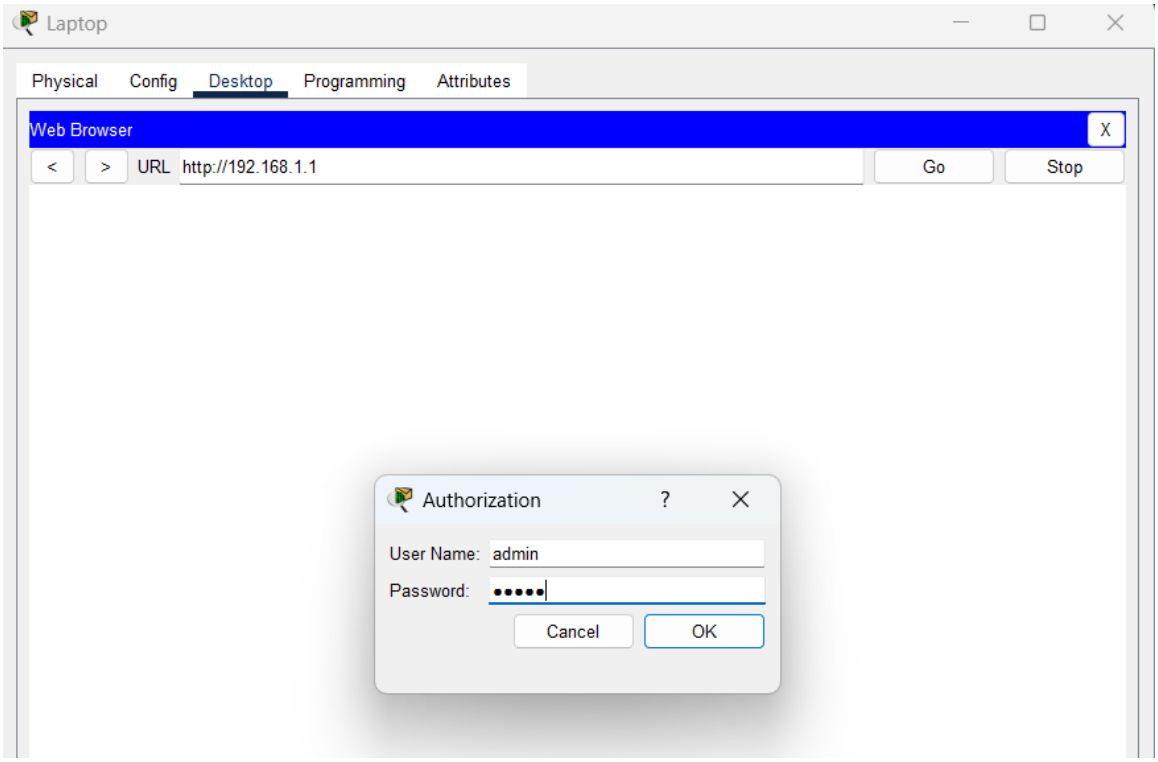
Website loading before security

5. Part 2 – Configure WPA2 Personal on the Wireless Router

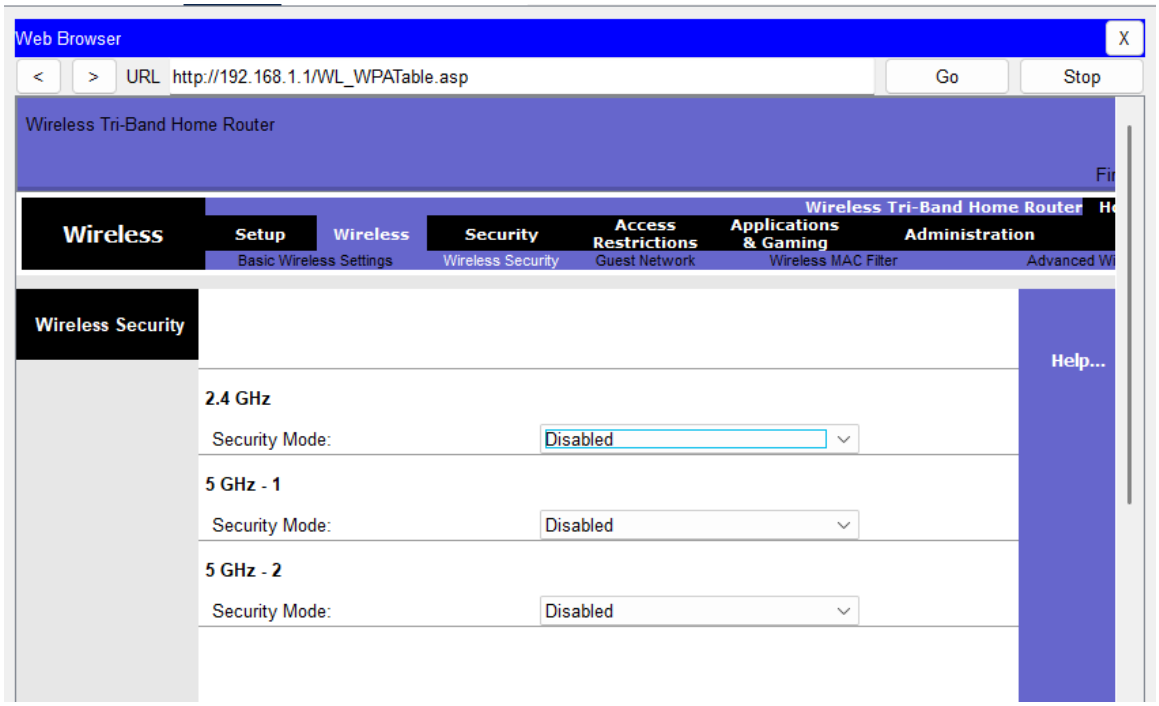
To secure the wireless network, WPA2 Personal was configured on the wireless router. WPA2 Personal uses a pre-shared key (PSK) and strong encryption to protect wireless traffic.

Steps performed:

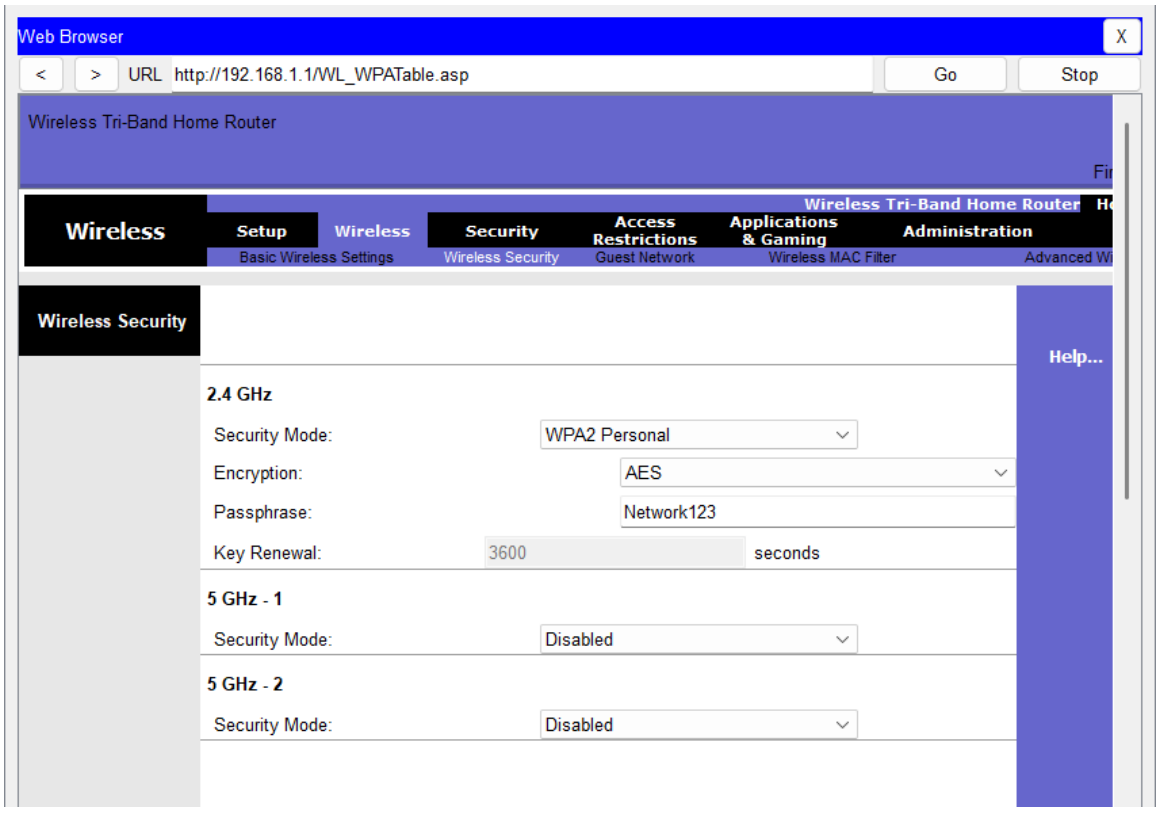
1. Opened the Web Browser on the laptop
2. Navigated to 192.168.1.1
3. Logged in using admin/admin credentials



4. Selected the Wireless menu
5. Opened Wireless Security settings



6. Set Security Mode to WPA2 Personal (2.4 GHz)
7. Entered Network123 as the passphrase
8. Saved the settings



Router wireless security settings

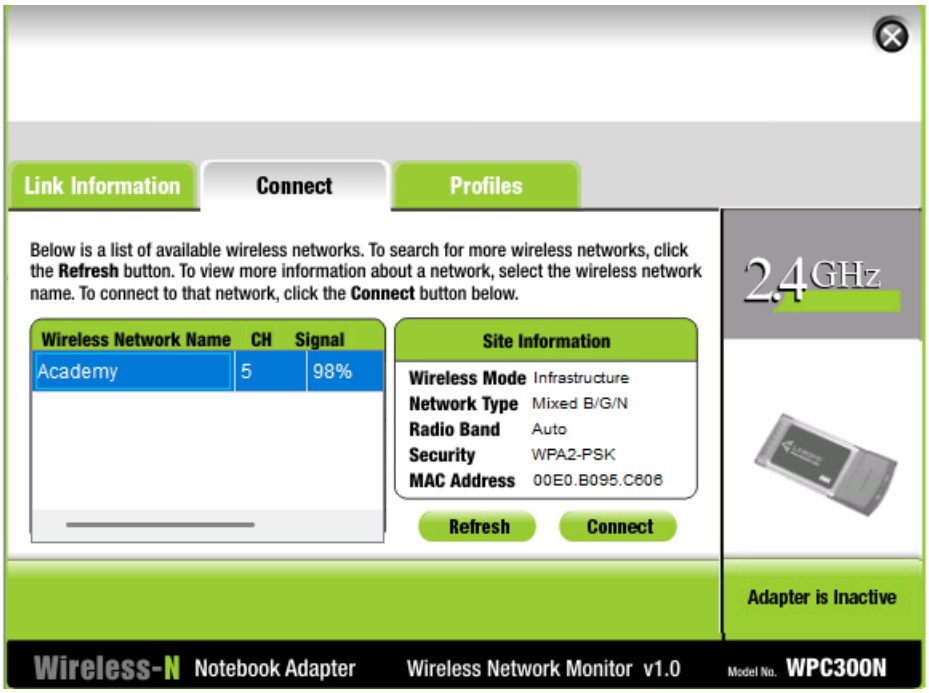
6. Part 3 – Update Laptop Wireless Settings

After enabling WPA2 security, the laptop was required to reconnect to the wireless network using the configured pre-shared key.

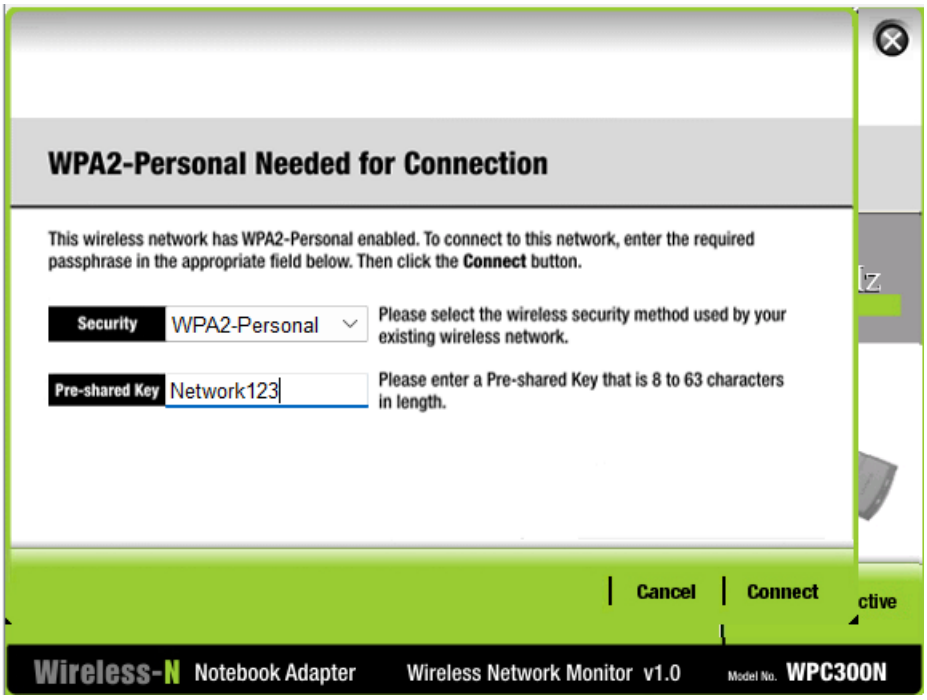
Steps performed:

1. Opened PC Wireless from the Desktop tab

2. Selected the Academy wireless network
3. Clicked Connect



4. Entered Network123 as the security key
5. Successfully connected to the secured network

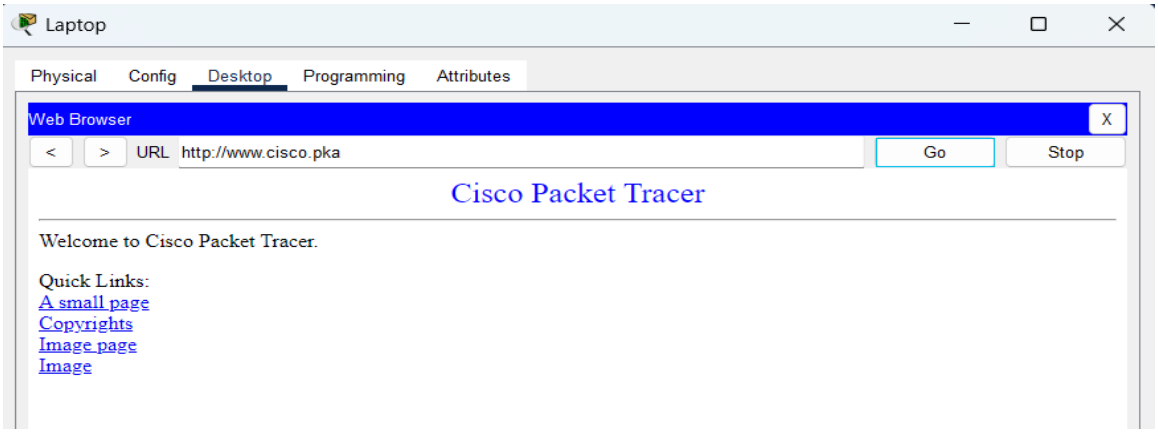


Laptop connecting to secured Wi-Fi

7. Part 4 – Verify Connectivity (After Security)

After the wireless network was secured and the laptop reconnected, connectivity was tested again to ensure normal operation.

Steps performed:
1. Opened the Web Browser
2. Entered www.cisco.pka
3. Confirmed the webpage loaded successfully



Website loading after WPA2 security

8. Security Explanation

WPA2 Personal secures the wireless network by encrypting traffic between the router and clients. Only devices that know the correct pre-shared key can join the network. This prevents unauthorized users from accessing internal resources or intercepting wireless traffic.

9. Reflection

This lab highlights the importance of wireless security in small business environments. Leaving a wireless network open exposes it to unauthorized access and potential attacks. By implementing WPA2 Personal, the network becomes significantly more secure without adding complex configuration.