Project Business Context:

Low-Cost RF & Wi-Fi Environment Monitoring System

1. Executive Summary

This project proposes the development of a low-cost, highly scalable network of sensors using ESP32 microcontrollers to actively monitor the Radio Frequency (RF) environment. In modern business, reliable Wi-Fi is not a-luxury - it is a critical utility. This system will provide continuous, real-time data on Wi-Fi channel congestion, signal strength, and interference. These actionable insights will empower IT teams to move from a reactive troubleshooting model to a proactive one, optimizing network performance, enhancing security, and significantly reducing the costs associated with diagnosing wireless issues.

2. The Business Problem

In any office, warehouse, or campus, Wi-Fi performance is directly tied to productivity. However, wireless networks are vulnerable to a wide range of invisible problems:

- **Productivity Loss:** Poor signal, "dead zones," and slow speeds directly halt work, frustrate employees, and lead to cumulative downtime.
- **High Troubleshooting Costs:** When a "bad Wi-Fi" complaint is filed, IT technicians must often spend hours with specialized, expensive equipment (like spectrum analyzers) to manually diagnose the problem. This is a costly, inefficient, and reactive process.
- **Performance Degradation:** The 2.4GHz and 5GHz bands are shared public frequencies. Interference from neighboring offices, personal hotspots, or even non-Wi-Fi devices (like microwaves or wireless peripherals) can degrade network quality without any obvious cause.
- **Security Vulnerabilities:** Unauthorized "Rogue Access Points" (e.g., an employee plugging in their own router) can create major security holes, bypassing corporate firewalls and exposing the internal network to attack. These are invisible to traditional network software.

Current professional-grade RF analysis tools are prohibitively expensive, costing thousands of dollars per unit. This makes it unfeasible to deploy them for continuous, building-wide monitoring.

3. The Proposed Solution

This project will create a distributed monitoring system using inexpensive, off-the-shelf ESP32 hardware.

- **Distributed Sensors:** Multiple ESP32 devices will be deployed across the target environment (e.g., one per floor, or one per high-priority zone like a conference room).
- **Continuous Scanning:** Each sensor will be programmed to continuously scan the 2.4GHz and 5GHz Wi-Fi bands.
- **Data Collection:** The sensors will capture key metrics for all nearby access points, including:
  - SSID (Network Name)
  - RSSI (Received Signal Strength Indication) - Tells you "how loud" the signal is.

    - Operating Channel - Tells you which "lane" of the frequency they are using.
    - MAC Address (Device ID)
- **Centralized Dashboard (Future Scope):** The data from all sensors will be aggregated and sent to a central database. This data will then be visualized on a simple web dashboard, providing a real-time "health map" of the entire wireless environment.

4. Business Value & Objectives

This solution directly translates a technical capability into measurable business value.

- **Objective: Reduce Operational Costs**
    - Value: Drastically lower the capital expenditure (CAPEX) for network monitoring by replacing multi-thousand-dollar analyzers with sub-$20 ESP32 devices. Reduce operational expenditure (OPEX) by cutting down on manual troubleshooting time.
- **Objective: Improve Productivity & User Experience**
    - Value**:** By identifying areas of high channel congestion or poor signal, IT can proactively optimize the network (e.g., change an AP's channel) before users experience problems, ensuring consistent, reliable connectivity.
- **Objective: Enhance Network Security**
    - Value: The system can be programmed to instantly flag any unauthorized or "rogue" SSIDs that appear on the network, alerting the security team to a potential breach in real-time.
- **Objective: Optimize Infrastructure ROI**
    - Value: Provide concrete data to justify network hardware upgrades or changes. The system can prove why a new access point is needed in a specific "dead zone," ensuring technology budgets are spent effectively.

5. Target Stakeholders & User Stories

This section details the primary users of the system and their specific needs.

- **IT Administrators & Helpdesk:** The primary users. This tool will be their first-line-of-defense for diagnosing all "bad Wi-Fi" complaints.
    - As an IT Helpdesk Technician, I want to view the live signal strength and channel usage for a specific user's location so that I can immediately determine if their "bad Wi-Fi" complaint is related to interference or a dead zone.
    - As an IT Helpdesk Technician, I want to see a list of all detected Access Points in a specific area so that I can identify which AP a user's device is (or should be) connecting to.
- **Network Operations (NetOps) Team:** Will use the aggregated data to analyze long-term trends, plan for network capacity, and optimize the entire wireless infrastructure.
    - As a NetOps Engineer, I want to see a historical graph of channel congestion for the 2.4GHz band in the main conference room so that I can decide whether to move more devices to 5GHz.
    - As a NetOps Engineer, I want to see a heatmap of signal strength across the entire floor plan so that I can identify "dead zones" and plan the location for a new Access Point.
    - As a NetOps Engineer, I want to view a report of RSSI values over time for our critical APs so that I can optimize their transmit power and roaming behavior.
- **Cybersecurity Team:** Will use the system as a "rogue AP" detection and alert system.

    - As a Cybersecurity Analyst, I want to receive an immediate alert when a new, non-corporate SSID is detected broadcasting within our facility so that I can investigate a potential rogue AP.
    - As a Cybersecurity Analyst, I want to maintain a "whitelist" of all approved corporate SSIDs and BSSIDs (MAC addresses) so that the system can automatically flag any device not on that list.
- **Facility Management:** Can use signal strength data to understand how new construction or office layouts might impact wireless coverage.
    - As a Facility Manager, I want to compare the Wi-Fi signal strength map before and after installing new glass-walled offices so that I can see if the new construction is blocking the signal and advise IT.

6. Key Use Cases

This section describes practical, scenario-based examples of the system in action.

- **Use Case 1: Troubleshooting a "Bad Wi-Fi" Complaint**
    - User: IT Helpdesk Technician
    - Scenario: A user in the 3rd-floor marketing-pod reports "the Wi-Fi is terrible."
    - Action: The technician opens the monitoring dashboard and filters for the sensor nearest to the user's location.
    - Insight: The dashboard immediately shows that channel 6 (2.4GHz) is extremely congested with 15+ networks, including several from a neighboring office. It also shows the user's corporate AP (SSID: "CorpNet") has a weak signal (-78 dBm) in that specific area.
    - Result: Instead of a 2-hour site visit, the technician logs a ticket for the NetOps team to investigate changing the AP's channel on the 3rd floor and to check the AP's placement or power level. The problem is diagnosed in 5 minutes.
- **Use Case 2: Proactive Network Optimization**
    - User: NetOps Engineer
    - Scenario: The NetOps team is planning for the next quarter's budget.
    - Action: The engineer pulls a 30-day historical report from the dashboard, looking at the signal strength heatmap for the entire campus.
    - Insight: The data clearly shows a "dead zone" (RSSI < -80 dBm) in a newly configured employee lounge area. It also shows that the main conference room's 2.4GHz channels are consistently at 90% utilization between 2 PM and 4 PM.
    - Result: The engineer submits a budget request for one new AP in the lounge, providing the heatmap as justification. They also reconfigure the conference room AP to more aggressively push clients to the 5GHz band, resolving the congestion issue before it generates more complaints.
- **Use Case 3: Real-Time Security Alert (Rogue AP)**
    - User: Cybersecurity Analyst
    - Scenario: An employee, frustrated with the Wi-Fi, brings in their own wireless router from home and plugs it into a live network port in their office.
    - Action: Within 5 minutes, the nearest ESP32 sensor detects a new SSID ("Steve's-Internet") that is not on the corporate "whitelist."
    - Insight: The system automatically flags this as a "Potential Rogue AP" and sends an alert to the cybersecurity team's dashboard, including the MAC address of the device and the sensor that detected it (pinpointing its physical location).

    - Result: The security team is able to find and disconnect the unauthorized device in minutes, closing a major security hole before it can be exploited.
- **Use Case 4: Validating Facility Changes**
    - User: Facility Manager
    - Scenario: The company is about to install a new set of floor-to-ceiling glass walls to create a new executive office.
    - Action: The Facility Manager consults with IT. The NetOps team runs a "baseline" report on the area's signal strength for 48 hours before construction.
    - Insight: After the glass is installed, the team runs the report again. The data comparison shows a 15 dBm signal drop inside the new office, confirming the glass is blocking the Wi-Fi signal.
    - Result: Because this was anticipated, IT had already planned to install a new, low-power AP inside the new office, which is done immediately. There are zero complaints from the executive on their first day in the new office.