Dedicated Scan Radio Technology White Paper

Contents

1 Overview

RF (Radio Frequency) scanning describes the process of analyzing the radio-frequency environment. Dedicated RF scanning is a core innovation in next-generation enterprise wireless networks.

With dedicated RF scanning, access points can simultaneously monitor 2.4 GHz, 5 GHz, and 6 GHz bands. Equipped with this capability, APs perform spectrum analysis of their surrounding environment without impacting production traffic. This enables real-time detection of rogue devices, channel interference, and security threats.

This white paper outlines the technical architecture, and application cases to help enterprises build highly reliable, self-defending intelligent wireless networks.

1.1 Introduction

Dedicated RF scanning—centered on interference detection and spectrum analysis—is designed as the foundation for a high-reliability, always-aware enterprise wireless network. Its core value lies in:

- **Zero Service Interruptions:** A physically isolated scanning RF chip ensures uninterrupted data transmission, eliminating latency and packet loss risks for mission-critical applications.
- **Panoramic Monitoring:** Concurrent scanning across 2.4 GHz, 5 GHz, and 6 GHz enables full-spectrum visibility for Wi-Fi 6E/7, closing security gaps in emerging bands and creating a complete interference map of the wireless environment.
- **Self-Diagnosis:** A dedicated packet capture channel collects over-the-air frames transmitted by the primary RF, enabling APs to diagnose their own failures—something traditional devices cannot achieve.
- **Integrated Defense and Operations:** By combining threat detection with spectrum scanning, the solution forms a closed loop of sense–analyze–act, dramatically reducing operational complexity.

By enabling a "zero-disruption diagnostic engine," dedicated RF scanning transforms enterprise operations from reactive "offline troubleshooting" to proactive "online precision diagnostics."

1.2 Background

With the rise of Wi-Fi 6/7 and the rapid growth of IoT, enterprise wireless networks face critical challenges:

- **Forced Service Interruptions:** Traditional scanning relies on switching the primary

RF into scan mode, cutting off user traffic. For latency-sensitive applications, this leads to packet loss and severe service disruption.

- **Blind Spots in Multi-Band Monitoring:** A single RF design cannot simultaneously scan 2.4 GHz, 5 GHz, and 6 GHz. Interference across different bands cannot be continuously monitored.
- **Complex Troubleshooting:** When the RF module in a traditional AP fails, diagnosis depends on other devices to capture over-the-air packets. Self-diagnosis isn't possible.
- **Poor Adaptation to Dynamic Environments:** One-time scans cannot adapt to changing network topologies, fluctuating traffic, or shifting interference sources. Traditional solutions lack real-time awareness.

Dedicated RF scanning solves these pain points through physical isolation and panoramic tri-band scanning, ensuring zero service disruption while delivering end-to-end security visibility.

1.3 Purpose of this White Paper

This white paper aims to:

1. Explain the principles and advantages of dedicated RF scanning.
2. Share best practices from real deployments.
3. Highlight applications across different enterprise scenarios.
4. Enable enterprises to build intelligent wireless networks with seamless service, self-diagnosis, and automated optimization.

2 Introduction of Key Technologies

2.1 Basic Concepts

By deploying a dedicated scanning RF chip that operates independently from the primary business RF, networks can continuously sense the entire wireless spectrum and detect threats without disrupting live traffic. Traditional solutions rely on time-sharing scans on the main RF, often causing latency spikes and critical interruptions.

2.2 Technical Advantages

Network Stability: Dedicated scanning radios operate non-intrusively by continuously monitoring environmental over-the-air packets and spectrum interference, while main-radio-based scanning increases network latency and risks service disruption.

Multi-Band Scanning: Dedicated RF chips enable dynamic switching across 2.4 GHz/5

GHz/6 GHz frequencies, allowing tri-band spectrum coverage with a single chip to detect environmental anomalies and eliminate security blind spots.

Self-Diagnosis Capability: Devices equipped with dedicated scanning radios can perform self-diagnosis of main-radio faults without relying on external packet capture tools.

2.3 Market Demand

As enterprise-level wireless networks evolve toward Wi-Fi 7 and IoT devices undergo large-scale deployment, traditional main-radio-dependent scanning solutions face fundamental challenges. First, switching the main radio to scanning mode disrupts live traffic, making it intolerable for latency-sensitive networks and blocking self-diagnosis during over-the-air fault detection. Second, these solutions cannot achieve tri-band (2.4 GHz/5 GHz/6 GHz) full-spectrum coverage with a single chip. Consequently, dedicated RF scanning technology has emerged as a reliable solution for zero service interruption and 24/7 network observability.

3 Key technical principles

3.1 Protocol Analysis

IEEE 802.11 is a set of standards developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networks (WLANs), commonly known as Wi-Fi. It defines the physical layer and medium access control (MAC) layer specifications that enable wireless devices to communicate over radio frequencies such as 2.4 GHz, 5 GHz, and 6 GHz. The 802.11 family supports multiple versions (including 802.11n, 802.11ac, and 802.11ax) to improve data rates, efficiency, and reliability, and is widely used in homes, enterprises, and public networks.

The format of an 802.11 frame is as follows:

Frame Control	Duration ID	Address 1 receiver	Address 2 sender	Address 3 filtering	Seq-ctl	Address 4 Optional	Frame Body	FCS
2Byte	2Byte	6Byte	6Byte	6Byte	2Byte	6Byte	0-2312Byte	4Byte

Alt text：Structure of 802.11 frames.

The fields are defined as follows:

1. **Frame Control:** This field contains several identification bits, indicating the frame type and other information.

2. **Duration ID:** This field contains the duration and ID bits and occupies two bytes (16

bits).

3. **Address:** Unlike the 802.3 Ethernet transmission mechanism, 802.11 wireless LAN data frames can have a total of four MAC addresses: the first is the receiver, the second the sender, and the third the filtering address.

4. **Seq-ctl:** This field is used to reassemble fragmented data frames and discard duplicate frames.

5. **Frame Body:** This field contains the data packets.

6. **FCS:** This field is used to check frame integrity.

3.2 Principle Analysis

3.2.1 Wi-Fi Interference Scanning

Wi-Fi scanning is a core technology for wireless network analysis and the foundation of wireless network connectivity. Essentially, it acquires information about surrounding networks by listening to radio frequency channels and uses the information for network connection and interference detection. Depending on how it works, there are two main mechanisms: active scanning and passive scanning. Each mechanism has significant differences in efficiency and network impact.

Active Scanning

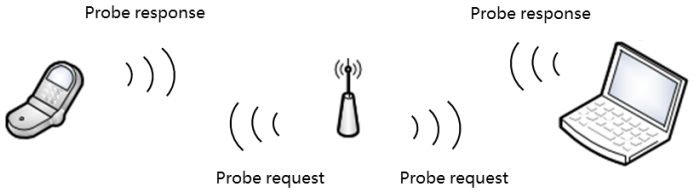
The core of active scanning lies in its interactive detection mechanism, which relies on an AP proactively sending Probe Request frames.

When scanning is initiated, the AP broadcasts Probe Request frames (destination address FF:FF:FF:FF:FF:FF) over the air, channel by channel, according to a predefined list. After a specified dwell time, it transitions to the next channel. The Probe Request frames carry the device's supported rate set and capability parameters.

Upon receiving the Probe Request, nearby APs respond with Probe Response frames on the same channel based on the 802.11 protocol. These frames contain key information similar to beacon frames, including BSSID, SSID, supported rates, and security policies. This information allows the device to identify the characteristics of other APs in the surrounding environment and identify interference and security threats.

Active scanning is implemented through interactive probing, which typically involves relatively fast message transmission. Therefore, the channel dwell time does not need to be excessively long. However, the channel dwell time is defined by each vendor and is not completely fixed. For example, with a typical channel dwell period of 100 ms per channel, a full scan on the 2.4 GHz band takes approximately 1.5 seconds. Its advantage lies in its fast response time, which can force APs with hidden SSIDs to become visible (since APs must

respond to targeted Probe Requests). However, frequently sending probe frames can significantly increase air interface noise.



Alt text：The process of Active Scanning.

Passive Scanning

Passive scanning uses a silent listening strategy to acquire 802.11 frames in the environment. The AP switches the radio to listening mode and continuously captures management frames on the channel without transmitting any data. Its core goal is to capture beacon frames periodically broadcast by surrounding APs (at a default interval of approximately 100 ms). These frames carry a complete network fingerprint: BSSID (AP MAC address), SSID (network name), channel number, RSSI (received signal strength index), encryption method (such as the WPA3 flag), and network load parameters (calculated using the Duration/NAV fields in the beacon).

Passive scanning does not require the AP to actively transmit signals, resulting in near-zero interference on the air interface, making it particularly suitable for covert surveillance scenarios. However, its efficiency is limited by the beacon broadcast interval. In low-density environments, to ensure that all AP beacons are captured, APs typically need to dwell on each channel for a longer period of time to capture every beacon frame. For example, if each channel requires a 300 ms dwell time, a full scan of the 6 GHz band can take 10 or more seconds.

Alt text：The process of Passive Scanning.

3.2.2 Spectrum Analysis

Spectrum Scanning

Spectrum scanning, similar to a simple spectrum analyzer, converts over-the-air electromagnetic signals into a visual format, helping users understand channel quality and interference distribution. This technology's implementation process consists of three stages:

First, electromagnetic signal acquisition is performed. The signal enters the device and undergoes hardware processing. A high-speed analog-to-digital converter (ADC) converts the analog signal into a digital sequence at thousands of samples per second.

After data acquisition, spectrum data conversion is required. The digital signal processor (DSP) performs a fast Fourier transform (FFT) on the sampled data, decomposing the time-domain waveform into a frequency-domain energy distribution.

Finally, visualization is performed. The processed spectrum data is presented as a dynamic spectrum heatmap: the horizontal axis shows continuous frequency points from 2401 to 7125 MHz, and the vertical axis displays signal strength from -110 dBm to -30 dBm. Color depth indicates the probability of signal strength at that location.

The spectrum graph helps users to identify interference. For example, if narrowband interference persists for a long time, a distinct spike will appear on the spectrum graph. The user can locate the source of the problem by observing the distribution of color blocks. If there is a continuous red area with high signal strength, avoid the channel.

Air Interface Packet Capture

The core of air interface packet capture lies in placing the wireless network card in monitor mode. This establishes a dedicated monitor interface to passively receive all RF signals on a designated wireless channel.

When the monitor interface is activated and configured for the specified channel, the wireless network card's underlying hardware and driver disable conventional MAC layer frame filtering. This means the card no longer receives only packets addressed to itself or broadcast/multicast packets. Instead, it captures all 802.11 protocol frames (including management frames, control frames, and data frames) detected by the radio chip at the physical layer of the channel, regardless of the destination address or network.

The driver then performs physical layer parsing on the captured raw RF signals, converting them into raw 802.11 MAC frames that can be processed via software. These frames contain the complete 802.11 frame header information.

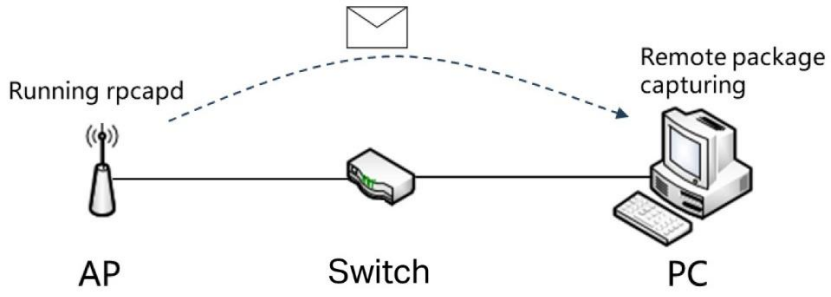
Ultimately, these complete packets, including the raw 802.11 frame content and physical layer metadata, are directly fed into the kernel's network protocol stack via the monitor interface, where they can be received, parsed, and stored by the user.

The entire process is completely passive; the monitoring device itself does not transmit any data that could interfere with normal wireless communication.

3.2.3 Streaming Mode Packet Capture

Unlike local packet capture, which requires saving the captured data in a pcap file and

downloading it locally, streaming packet capture lets you remotely monitor the AP's interface with tools like Wireshark, displaying the captured packets in real time. Streaming packet capture primarily uses the open-source rpcapd utility to transfer captured data from the AP to Wireshark on your PC.



Alt text：The process of Packet Capture

Serving as a bridge between the AP and the PC, the rpcapd process communicates with both parties as follows:

After establishing a connection with Wireshark, the two parties first authenticate depending on the type of rpcap packet being sent. rpcapd verifies Wireshark's identity.

After authentication, Wireshark requests access to all interfaces on the AP. Wireshark then requests to open a capture session. rpcapd accepts and opens the session, setting basic information such as the capture interface and the capture length.

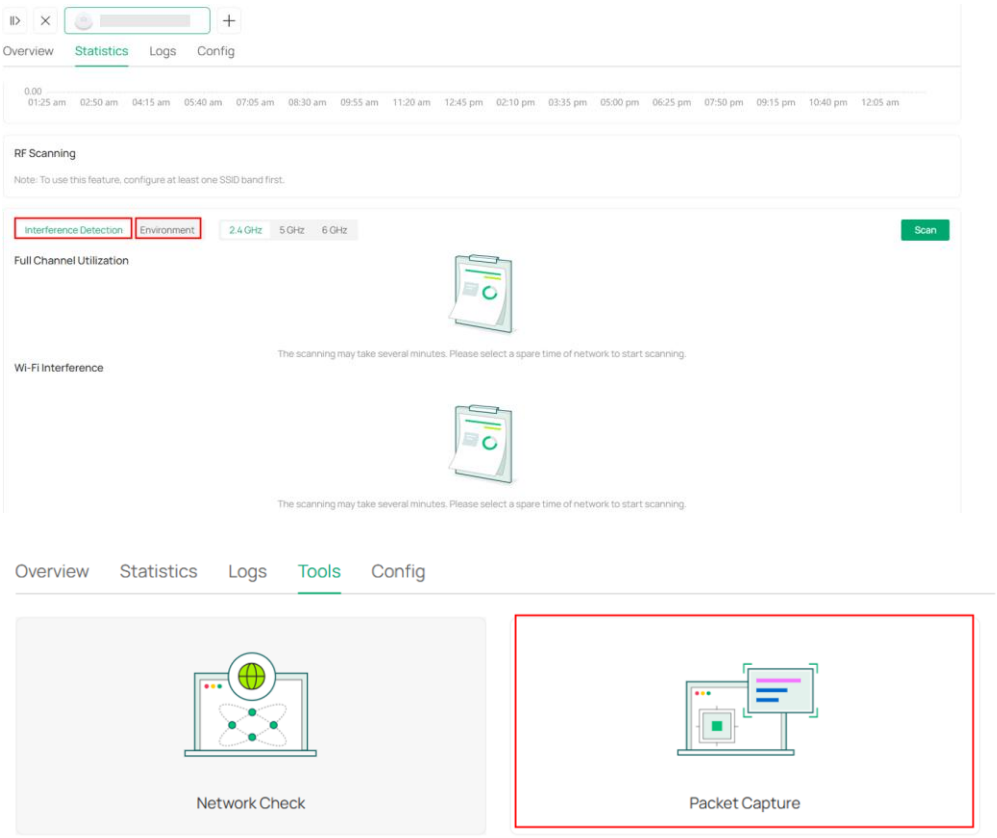
Once ready, when Wireshark requests to begin capturing, rpcapd receives the request and calls the AP's monitor interface to begin capturing. To terminate capture, Wireshark also initiates a request, which rpcapd then completes. During the capture process, rpcapd sends captured data packets to Wireshark in real time. Wireshark parses the data and displays it in real time.

rpcapd does not save data locally. Therefore, when capturing packets in stream mode, you do not need to consider the size of the captured packet file.

3.3 Frame Analysis

In Omada AP products, the following three features are implemented through independent RF chips:

- **Interference Detection**
- **Environment**
- **Wireless Packet Capture**



Alt text: Dedicated RF Scanning features in Omada Controller.

Note that the RF Scanning in the picture is not part of this feature set. RF Scanning is currently implemented through the main RF chip on all APs, and performing this function will cause wireless clients to disconnect from the network temporarily.

3.4 Application Scenario Analysis

Dedicated RF scanning is widely applied in scenarios such as wireless network planning and optimization, interference detection, wireless monitoring and complex industrial or public environments. By providing real-time insight into signal strength, channel usage, and anomalous transmissions. Dedicated RF scanning supports reliable wireless system operation, interference mitigation, and efficient spectrum utilization.

4 Application Scenarios & Solutions

4.1 Interference Detection & Optimization

When issues such as sudden speed drops, frequent disconnections, or increased latency occur, it might be due to new interference sources in the environment. For such cases, use Scan-Radio's interference detection feature to acquire Wi-Fi interference sources,

channel utilization data, and non-Wi-Fi interferences across the environment. For deployments with three or more APs, it enables interference source localization. Operators can then optimize network layouts or remove interference sources to restore Wi-Fi performance.

The following FAQs introduce methods for detecting interference in Omada Controller:

- Interference Detection on Omada Controller | Omada Network Support
- How to Capture Wireless Packets via EAP and Omada Controller | Omada Network Support

4.2 Spectrum Planning & Deployment

Pre-deployment electromagnetic environment assessment is critical in ports, factories, and similar scenarios to avoid frequency conflicts. During network planning, use Scan-Radio's Spectrum Scanning (Environment) feature to scan target areas to:

- Identify underutilized frequency bands
- Measure baseline noise and signal distortion levels
- Model potential interference patterns

This feature can enhance deployment efficiency while reducing post-deployment optimization costs. For example, you can use Scan-Radio for environmental scanning to detect interferences and identify available frequency bands.

4.3 Autonomous Network Performance Optimization

Conflicts between newly deployed APs and existing infrastructure, or sudden environmental interference sources, often lead to network performance degradation and client roaming failures. Manual reconfiguration is not only time-consuming but also requires preliminary interference identification. Scan-Radio's auto-deployment capability addresses this by autonomously optimizing AP configurations—including channel, bandwidth, frequency band, and transmit power—to achieve intelligent network performance tuning.

Common Wi-Fi issues such as client association failures or roaming disruptions often require over-the-air (OTA) packet analysis between clients and APs. Traditional approaches rely on specialized packet capture tools or macOS-based solutions, creating technical or device-related barriers for common users.

Moreover, changing channel configurations during packet capture often disrupts live networks. With Scan-Radio, the dedicated RF chip enables background scanning without affecting foreground services—no software upgrades or network reconfiguration required.

4.4 Case Analysis

Client Roaming Failure Troubleshooting

A client reported that a specific model of smartphone failed to roam properly between EAPs. To diagnose the issue, the R&D team provided the client with a dedicated packet capture firmware to collect OTA packets, alongside technical guidance. However, if the client's device supports native OTA packet capture and the management software provides built-in configuration, the client can independently collect and submit diagnostic data for after-sales analysis, reducing R&D resource demands.

Bridge Product Interference Mitigation

A client experienced suboptimal performance with EAP215-Bridge devices over an 800-meter inter-building link, achieving only 20Mbps throughput on an 80MHz channel. Meanwhile, the devices failed to establish connections. Initial technical support suspected urban environmental interference but lacked on-site detection tools for confirmation. With Scan-Radio's interference detection and localization capabilities, this problem could have been identified and avoided.

Large-Scale Mesh Network Optimization

A client observed excessive WPA authentication attempts in their controller logs, which technical analysis attributed to coverage blind spots. However, traditional RF scanning and WLAN optimization tools are incompatible in a dense mesh environment. Devices equipped with dedicated radio scanning chips can perform spectrum analysis and environmental assessments unaffected by mesh networking constraints, which enables automated optimization even in complex mesh deployments.

5 Representative Model

EAP 787 - BE15000 Ceiling Mount Tri-Band Wi-Fi 7 Access Point

Alt text：EAP 787

- **Dedicated RF Scanning:** Offers real-time spectrum monitoring and dynamic interference avoidance for robust wireless performance.[§]
- **Tri-Band 8-Stream Wi-Fi 7:** 5765 Mbps on 6 GHz, 8648 Mbps on 5 GHz, and 688 Mbps on 2.4 GHz.[†]
- **Low Latency and Interference:** 320MHz Bandwidth, Multi-Link Operation, Multi-RUs, and 4K-QAM ensure high performance for your network.‡
- **Advanced Features:** Supports centralized management, Mesh, and Seamless Roaming.
- **More Capacity and Wider Coverage:** Supports 510+ concurrent clients and covers up to 2050 ft² (190 m²) for reliable and extensive wireless connectivity.

If you want to know more, please go to EAP787 | BE15000 Ceiling Mount Tri-Band Wi-Fi 7 Access Point | Omada by TP-Link

6 Future Trends

Providing richer, more diverse, refined, and multi-terminal O&M services is a key direction to meet future advanced O&M requirements and technologies.

We foresee the following key directions:

1. **Refined and Diversified Interference Source Detection**

Currently, the Interference Detection function supports full channel occupancy detection and Wi-Fi interference source detection. Detection of non-Wi-Fi interference sources and refined identification of interference source types are not involved.

2. Comprehensive Management Platform

To meet the needs of performing O&M on different management platforms, Interference Detection, Environment, and Over-the-Air Packet Capture features will be gradually adapted to various management platforms (Software Controllers, Hardware Controllers, and Cloud-Based Controllers).

3. Scan-Radio Empowerment and Extension

With real-time scanning, Scan-Radio can provide powerful real-time data acquisition capabilities, improving and expanding the existing O&M capabilities to enrich or strengthen the current Q&M system.

7 Appendix

7.1 Glossary

Term	Full Name	Definition
BSSID	Basic Service Set Identifier	The physical address of an AP, uniquely identifying it within the same network.
SSID	Service Set Identifier	The name of a wireless network.
RSSI	Received Signal Strength Indicator	A measure of the wireless signal strength.
WPA3	Wi-Fi Protected Access 3	A modern network security and encryption protocol.
MAC	Media Access Control	The MAC layer address, usually referring to the physical address of a network card.
Beacon	Beacon	A special management frame periodically broadcast by an AP to advertise its presence and capabilities.
FFT	Fast Fourier Transform	An efficient algorithm that converts a signal from the time domain into the frequency domain.