



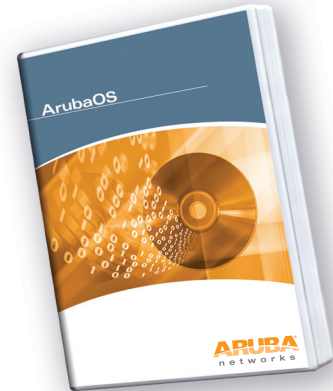
## ARUBAOS RFPROTECT MODULE

The ArubaOS RFProtect™ module is an optional software module installed on Aruba Mobility Controllers. RFProtect safeguards the network infrastructure against wireless security threats as well as provides a critical layer of visibility into sources of radio frequency (RF) interference and their effect on wireless LAN (WLAN) performance.

RFProtect provides the industry's only integrated wireless security and spectrum analysis system for enterprise WLANs and eliminates the need for a separate network of RF sensors and security appliances. Aruba's WLAN infrastructure allows access points (APs) to service WLAN clients while monitoring the air for interference sources and rogue devices. Aruba APs may also be turned into dedicated air monitors to focus on detecting and containing unauthorized APs and devices.

Additionally, any Aruba 802.11n AP may be configured as a spectrum analyzer to remotely scan 2.4- and 5-GHz radio bands, identify RF interference, classify the source and provide real-time analysis. With RFProtect, no specialized hardware or client software is required for RF spectrum analysis.

Used in conjunction with RFProtect, Aruba's AirWave Wireless Management Suite provides event history, event correlation, location tracking and security reports to meet compliance requirements, such as those defined by the Payment Card Industry (PCI).



### SPECTRUM ANALYSIS

RF interference in WLANs is inevitable and unpredictable. It can originate from neighboring Wi-Fi networks or non-Wi-Fi sources, such as 2.4-GHz cordless phones, microwave ovens, analog video cameras, gaming consoles and wireless telemetry systems. The characteristics and severity of RF interference varies based on the type and location of the device and may have an impact on client access and performance of the WLAN.

All Aruba 802.11n APs utilize Wi-Fi chipsets with integrated high-definition spectrum analysis capabilities, enabling always-on, simultaneous spectrum analysis and wireless security monitoring. Simultaneous scanning of the RF spectrum for interference and intrusion protection eliminates the cost and complexity of separate dedicated hardware or handheld analyzers with client software. As a result, the Aruba solution is less than half the cost of other products and reduces the time spent by IT staff to manually capture RF interference events.

The ArubaOS RFProtect module includes spectrum analysis capabilities used in conjunction with Aruba's Adaptive Radio Management (ARM) technology. RFProtect Spectrum Analyzer identifies and classifies interference sources in up to 13 categories, then provides administrator analysis of the interference via 12 graphical charts, including FFT and spectrogram graphs. Aruba's Adaptive Radio Management (ARM) employs infrastructure-based controls to optimize Wi-Fi client behavior and automatically ensures that APs stay clear of Wi-Fi and non-Wi-Fi interference.

### WIRELESS INTRUSION PROTECTION

Wireless networks make attractive targets for denial-of-service (DoS) and man-in-the-middle attacks. Aruba Mobility Controllers with RFProtect maintain signatures to identify and block

wireless attacks so service is not disrupted. Based on location signatures and client classification, Aruba access points will drop illegal requests and generate alerts to notify administrators of an attack.

Aruba APs monitor the air to detect other wireless stations masquerading as valid APs. RFProtect tracks unique signatures for each wireless client in the network. If a newly-introduced station claims to be a particular client but lacks a proper signature, a station impersonation or man-in-the-middle attack is declared. When a man-in-the-middle or invalid/masquerading AP is detected, defense mechanisms are put in place to contain the unauthorized device and prevent the corruption or loss of confidential data.

### CLASSIFYING AND DISABLING ROGUE ACCESS POINTS

Classification is the first step in securing the corporate environment from unauthorized wireless access. Adequate measures to quickly shut down intrusions are critical to protect sensitive information and network resources. APs and stations must be accurately classified to determine whether they are valid, rogue or neighboring APs, and an automated response must be implemented to prevent possible intrusion attempts.

With RFProtect, Aruba 802.11n APs support TotalWatch™ – the ability to scan all channels of the RF spectrum, including 2.4- and 5-GHz bands as well as the 4.9-GHz public safety band. TotalWatch also provides 5-MHz granular channel scanning of bands for rogue devices, and dynamic scanning dwell times to focus on those channels with traffic. TotalWatch provides an advanced set of features to detect unauthorized wireless devices and a set of customizable rules are utilized to highlight devices that truly pose a threat to the network.

# ARUBAOS RFPROTECT MODULE

Detected devices classified as rogues may be contained by forcing client association to a fake channel or BSSID. This method of tarpitting is more efficient than rogue containment via repeated de-authorization requests. Network administrators are notified of rogue devices, and the physical location of the rogue may be determined with the use of the AirWave.

RFPProtect will stop wireless traffic from flowing into the wired infrastructure via rogue APs, protecting the wired network against wireless security breaches.

## POLICY DEFINITION AND ENFORCEMENT

RFPProtect enables the configuration and dynamic enforcement of network policies. Examples of wireless policies include valid station protection, AP misconfiguration protection, ad-hoc network detection and protection, unauthorized network interface card (NIC) detection, and wireless bridge detection. RFPProtect includes a policy-configuration wizard, simplifying the creation of an organization's wireless security policies.

## RFPROTECT FEATURES

### SPECTRUM ANALYZER

Simultaneous RF spectrum analysis and security scanning

Integrated into all Aruba 802.11n APs

Scans 2.4- and 5-GHz bands

Classification of interference in up to 13 categories including:

- Bluetooth devices
- Cordless phone, network and base station devices
- Fixed-frequency video and audio devices
- Microwaves

Visualization via 12 spectrum analysis charts including:

- FFT Duty Cycle
- Real-time FFT
- Swept Spectrogram

Location tracking via AirWave Wireless Management Suite

### TOTALWATCH AIR MONITORING

Scanning of all bands (2.4-, 5- and 4.9-GHz public safety band)

Granular 5-MHz channel scanning

Dynamic dwell times

- 500 ms per channel with traffic
- 250 ms for channel within local regulatory domain

Intrusion protection configuration rules wizard

Security threat management visualization

Security alert events correlation

### ROGUE IDENTIFICATION AND CONTAINMENT

Granular 5-MHz scanning to detect rogues in between channels

Scanning of the 4.9-GHz public safety band

Automatic rule-based rogue classification

Wireless containment via fake channel/BSSID (tarpitting)

Wired containment via ARP poisoning and port disable with AirWave

Location tracking via AirWave

### IMPERSONATION DETECTION AND PREVENTION

Hotspotter attack detection

MAC address spoofing

AP impersonations

Man-in-the-middle attacks

Sequence number anomaly detection

### CLIENT INTRUSION PREVENTION

Honeytrap AP protection

Valid station protection

### DENIAL OF SERVICE ATTACK DETECTION

Auto immune attacks

Management frame floods

De-authentication attacks

Authentication floods

Probe request floods

Fake AP floods

Null probe responses

EAP handshake floods

### PROBING AND NETWORK DISCOVERY

Detection of NetStumbler and broadcast probes

### NETWORK INTRUSION DETECTION

Wireless bridges

ASLEAP attacks

### ORDERING INFORMATION

RFPProtect is available as a license for mobility controllers and is ordered based on the number of APs supported by the controller.

LIC-RFP-xx

RFPProtect Module License



[WWW.ARUBANETWORKS.COM](http://www.arubanetworks.com) | 1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)