



# APPLICATION BRIEF AirWave® RAPIDS™ Rogue Detection

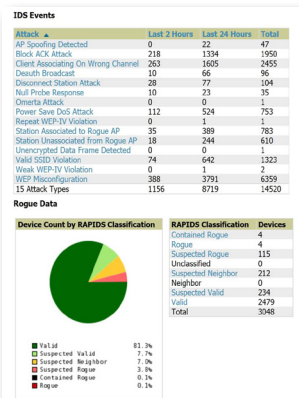
## Wired and Wireless Rogue Detection

AirWave RAPIDS™ Rogue Detection automatically detects and locates unauthorized clients and access points, and utilizes a set of rules to highlight the most important threats to your organization. RAPIDS uses existing, authorized APs to scan the RF environment for any unauthorized devices in range. It also scans your wired network to determine if the wirelessly detected rogues are physically connected to the local network, and to look for additional unauthorized devices in areas without wireless coverage. In addition, RAPIDS captures and manages IDS events detected by wireless LAN controllers. RAPIDS then correlates all of this data and uses a set of customizable rules to highlight those devices that are truly a threat to the organization, greatly reducing false-positives and allowing you to work more efficiently.

RAPIDS works in conjunction with the Aruba Networks Mobility Controller RFProtect software module to correlate and consolidate rogue AP and client, wired and wireless attack data, delivering a comprehensive Wireless Intrusion Protection Solution (WIPS). Customers can deploy this solution with “hybrid” APs serving as both APs and sensors or as an overlay architecture where Aruba APs act as dedicated sensors called air monitors (AMs). RAPIDS utilizes data from both the dedicated sensors and deployed APs to provide the most complete view of your wireless environment. The solution improves network security, manages compliance requirements and reduces the cost of manual security efforts.

### How Is RAPIDS Used?

As wireless LANs evolve into mission-critical infrastructure, organizations are becoming more concerned about managing network security in the most efficient manner. Most organizations implement strict policies banning the installation of unauthorized, or rogue, APs but often struggle



The RAPIDS dashboard gives network administrators and security personnel one place to view potential threats.

with enforcing these policies. In addition, a variety of compliance requirements such as those established by the Payment Card Industry (PCI) put greater pressure on organizations to reevaluate their WLAN strategy and operation. However, few enterprises have the tools or resources to adequately enforce their policies or follow up and resolve threats on a consistent basis. RAPIDS provides an efficient, effective process for rogue detection, correlation, classification, alerting, reporting and containment.

## The Aruba Advantage

### A Better User Experience

AirWave® from Aruba Networks has been designed from the ground up as a network operations solution for the whole IT organization, from the service desk, to the NOC, to network engineering. Each team member has role-based access to relevant information, and it's usually just a click or two away.

### User-Centric Management

AirWave gives you a single, accurate picture of everything that affects service quality for your users — from wired infrastructure, to the RF environment, to individual mobile devices. It also integrates easily with existing IT service management tools for more efficient problem resolution.

### Intelligence for Better Decision-Making

AirWave provides a wide range of actionable information, from time-sensitive alerts to historical reporting. With data that spans days, months and seasons, you always have the data needed to spot trends, plan capacity and craft the right strategies for your organization.

### Multi-Architecture, Multi-Generational

Even in mixed architecture networks with multiple generations of products, you have a single view to monitor and manage your entire network.

## Key Features

### WIRED NETWORK SCANS AND AP IDENTIFICATION

- Examines the MAC address of each device discovered by polling routers and switches and compares it to RAPIDS' database of 12,000+ known MAC address ranges to identify likely rogue devices
- Examines the MAC address of each device discovered by polling routers and switches and compares it to RAPIDS' database of 12,000+ known MAC address ranges to identify likely rogue devices
- Uses RAPIDS' database of 1,700+ OS types to identify the device operating system to help you eliminate false-positive results

### WIRELESS NETWORK SCANS

- Instructs authorized access points to scan the air for other wireless APs and clients
- Automatically builds a list of authorized APs to prevent them from being classified as rogues
- Allows you to distinguish between "true rogues" and "neighbor APs" that are in RF range but do not pose a threat to your network
- Displays valid and currently connected rogue clients, rogue client associations, and rogue client association history

### SCAN THE AIRSPACE OUTSIDE THE COVERAGE OF YOUR WIRELESS NETWORK

- Turns your existing wireless-enabled Windows devices into additional RF sensors with the optional AirWave Management Client™ (AMC) software

### WIRELESS INTRUSION DETECTION SYSTEM (WIDS) EVENTS

- Aggregates, correlates, alerts and logs wireless attacks that have been reported by your infrastructure, providing a full picture of your wireless network security

### COMPREHENSIVE RESULT CORRELATION

- Correlates information from wired and wireless scans, including SSID, RF channel, security method, radio MAC address or BSSID, network type, LAN MAC address, IP address and operating system
- Compares wired and wireless scans to eliminate duplicates and refine threat assessment

### RULES-BASED THREAT CLASSIFICATION

- Classifies potential threats based on rules you customize to define what a rogue device is
- Reduces false-positives and lets your security team focus on the most significant threats first

### AUTOMATED ALERTS AND REPORTS

- Assigns proper alert priority to each discovered AP and client depending on its classification
- Generates automated email alerts, syslog alerts, or SNMP traps containing all known information about rogue devices, including:
  - Radio MAC address
  - LAN MAC address
  - Discovery method
  - SSID
  - Channel
  - Security settings
  - Switch port
  - IP address
- Graphical dashboard displays real-time information on all suspected rogue APs and clients
- Pre-defined, customizable reports address common security and compliance information needs, such as rogue device tracking and PCI compliance

### VISUALIZATION

- Integrates with AirWave VisualRF™ to display the likely location of each rogue device on a building floor plan

### AUTOMATIC AND MANUAL CONTAINMENT

- Performs manual or automated rogue AP containment with Aruba and Cisco controllers
- Uses your customized rules-based classification scheme to determine when to automatically contain devices
- Can disable wired switch ports with rogue APs attached

APPLICATION BRIEF

## AirWave® RAPIDS™ Rogue Detection



[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)