RAPIDS™

ROGUE AP DETECTION MODULE

A More Intelligent Approach to Rogue AP Detection & Prevention

RAPIDS™ Product Overview

July 2005

Rogue Access Point (n.): 1) An unsecured wireless access point connected to the enterprise network by either well-meaning employees or malicious intruders without the knowledge or permission of the IT staff. 2) One of the most common threats to network security.

Unauthorized 'rogue' access points can expose sensitive corporate data to intruders and may undercut an organization's entire regulatory compliance program (Sarbanes-Oxley, HIPAA, CISP). With Wi-Fi access points readily available for less than $100 in any consumer electronics store, all organizations today *must* have a rogue AP detection strategy, regardless of whether they have installed authorized Wi-Fi networks.

Yet, many enterprises have failed to implement any defense against rogue access points. By combining wired and wireless (RF) detection techniques, AirWave's patent-pending RAPIDS™ software module provides a simple, easy-to-implement solution for these organizations. The RAPIDS software:

- **Provides effective rogue detection across your entire network**
- **Eliminates 'false positive' results**
- **Requires no costly RF sensors or specialized equipment**

"We calculated that it would take us two years to install wireless sensors in 3,000+ retail stores. Two years without a true security solution in place is far too long."

IT Security Manager, Fortune 500 Retailer

RAPIDS: A Multi-Faceted Approach

The measures of success for any rogue AP detection solution are: (1) Does it detect all rogue devices anywhere on the network?, and (2) Does it accurately eliminate false positive results to enable IT to focus on the real security threats?

There are two primary methods by which rogue access points can be detected. Wireless RF monitoring methods use Wi-Fi 'sensors' to detect other Wi-Fi devices within range. Wireline scanning solutions interrogate all devices connected to the wired network infrastructure to determine whether those devices are likely to be unauthorized access points.

	Wireless	Wireline
Advantage	Highly accurate rogue detection with a low false positive rate	Detect rogue devices anywhere on the network, without regard for physical proximity
Limitation	Only discover rogue devices within range of an RF sensor (typically ~200')	Difficult to detect all rogue APs via wireline scans without generating many false positives

An average Fortune 1000 corporation today has more than 600 physical locations and 35,000 employees (Source: U.S. Census Bureau). Very few organizations of this size have the wall-to-wall Wi-Fi network or RF sensor coverage that would allow them to detect *all* rogue APs via wireless means. Implementing this blanket RF coverage could cost millions of dollars and take several years to complete. As a result, the only cost-effective way for a large organization to successfully detect possible rogue APs across their entire network is to combine wireless (RF) monitoring with detection techniques from the wired side of the network.

Combining Three Powerful Rogue AP Discovery Techniques

AirWave's RAPIDS rogue detection software uses a unique combination of wireless and wireline scanning techniques. By using multiple techniques and leveraging the existing infrastructure rather than rather than requiring proprietary hardware, RAPIDS delivers highly effective rogue detection at a fraction of the cost of other solutions.

RAPIDS Overview

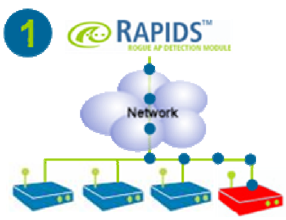
☑ 100% software solution with no proprietary hardware required

☑ Installs on standard PC server hardware

☑ Intuitive web-based user interface

☑ Linux OS for additional security

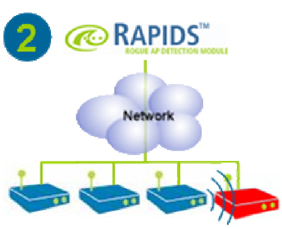
Wireline Rogue AP Detection



Wireline detection is the only method that can find rogue APs anywhere on the network, regardless of whether they are within range of existing access points or RF sensors. As such, it represents a baseline capability that every organization must have in place for effective enterprise-wide rogue detection – even if the organization has no wireless access points or sensors of its own.

AirWave Wireless has been providing multi-vendor wireless network management software since 2000. Through that unique experience, AirWave has developed the ability to automatically discover and definitively 'fingerprint' more than 100 access points from leading Wi-Fi hardware vendors, including Dlink, Linksys, Netgear, and others. Where a connected device cannot be fingerprinted with 100% certainty, the RAPIDS software also queries routers and edge switches to gather MAC address data for the device. RAPIDS then compares the MAC address with AirWave's continuously updated, proprietary database to determine whether it matches known addresses of Wi-Fi devices. When RAPIDS discovers a rogue AP via wireline detection, it can typically identify the switch port to which the rogue is connected.

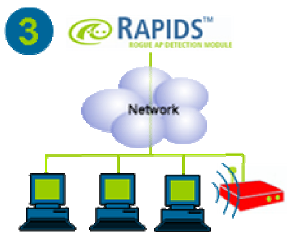
RF Scanning with Authorized Access Points



The most valuable source of real-time RF information in most enterprises is often the organization's authorized, managed wireless access points. Most enterprise-grade APs from leading vendors today have the ability to wirelessly scan their airspace and report all other Wi-Fi access points within range. The RAPIDS software remotely instructs the APs to initiate these RF scans and compares the resulting list of detected APs with its database of known APs to identify any unknown potential rogues. Wireless scanning via authorized APs is a highly effective means of detecting any rogues within range and has a very low 'false positive' rate. This method becomes increasingly effective as the organization's authorized wireless LAN infrastructure grows to encompass more APs capable of performing this RF scanning.

Wireless scanning via authorized APs is typically very cost-effective because it does not require proprietary software on the access points themselves. When used with RAPIDS, 'out-of-the-box' access points from vendors like ProCurve Networking by HP, Airespace, Avaya, Colubris, Intel, Proxim, Symbol and others vendors support RF scanning today. Cisco Aironet access points provide RF scanning data when used in conjunction with the Ciscoworks WLSE appliance. RAPIDS also contains an API for integration with third-party wireless IDS solutions to facilitate the use of these proprietary RF sensors where installed.

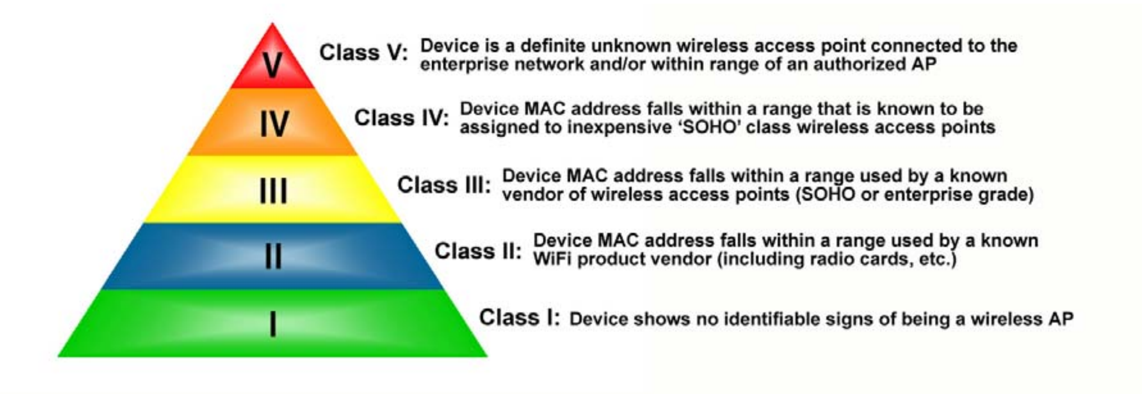
RF Scanning with Wi-Fi Enabled Client Devices



Since most organizations today do not have wall-to-wall Wi-Fi coverage with authorized access points, wireless detection solutions that rely exclusively on APs for RF detection may have large coverage gaps in their wireless scanning capacity. To address this problem, AirWave offers the optional, easy-to-use AirWave Management Client (AMC) software for Windows-based clients. The AMC software enables WiFi-enabled client devices to act as mobile RF sensors, reporting data on all APs within range. RAPIDS analyzes this client-reported data and correlates it with information from all other RF and wireline scans to identify any unknown, unmanaged APs within the airspace.

Filtering Potential Rogue APs to Eliminate False Positives

Rogue detection solutions that generate large numbers of false positive results can be even worse than having no solution at all, since IT can spend thousands of hours investigating false leads rather than working on real security problems. The RAPIDS software analyzes data from its multiple detection techniques to eliminate false positives and assign each device on the network a score from 1-5, reflecting the likelihood that the device is a rogue AP. A "Class V" RAPIDS score indicates that the devices is definitely an unknown AP that could be connected to the enterprise network, while a "Class I" RAPIDS score indicates that the device shows no signs of being a rogue.



Using RAPIDS' web-based user interface, the IT staff can specify when it wants to receive automated rogue AP alerts (i.e., "Alert when a potential rogue is discovered with a Class IV or greater), assign priority codes to these alerts ("Critical," Major", "Warning," etc.), and determine how the alerts are to be delivered (via email, SNMP trap, and/or onscreen console). RAPIDS rogue AP alerts contain all relevant data about the suspect rogue, including:

- Radio MAC
- LAN MAC
- Discovery Method (AP Scan, etc.)
- Discovery Time
- Discovery History
- SSID
- Security Settings
- Switch Port

The IT staff can filter possible rogue lists by Class and use this data to focus its limited resources on investigating the devices most likely to represent a real threat to network security.

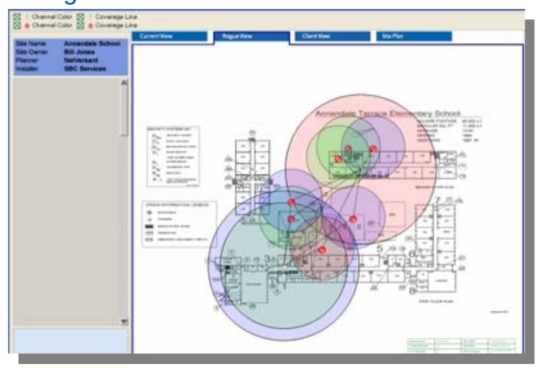
FACT: Using wireline detection alone, the RAPIDS software can accurately detect and classify all 100% of the top one hundred best-selling wireless APs sold on Amazon.com*, assigning them a score of Class IV or higher.

*(as of June 23, 2005)

Locating Rogue Access Points

RAPIDS provides several detailed reports to help the IT staff locate and remove suspected rogue APs quickly and efficiently. When a rogue is detected via wireless RF scans, RAPIDS uses relative signal strength (RSSI) values from the scanning APs or AirWave Management Client to triangulate the physical location of the possible rogue.

Rogue AP View within visualRF™



When RAPIDS is used in conjunction with AirWave's visualRF™ software module, it uses this RF data to calculate the rough physical location of a potential rogue on a map, allowing IT to dispatch local support staff to the correct location to investigate the unknown AP. If the suspected rogue is an innocent neighbor (i.e., an AP not connected to the enterprise network but still within RF range), IT can instruct RAPIDS to 'ignore' the device and not generate alerts when it is detected in the future. If the device is actually an unsecured rogue, the local support staff can quickly locate and physically remove it.

If RAPIDS detects the device via wireline scanning, it can typically provide data on the exact switch port to which the unauthorized rogue is connected:

Switch ^	Port	Time	Discovery Method
switch1.dev.airwave.com	50	6/24/2005 4:58 PM	Switch/Router MAC address scan
switch2.dev.airwave.com	37	6/24/2005 4:58 PM	Switch/Router MAC address scan

With this information, IT can typically remotely disconnect the device wherever it is located on the network.

For More Information

AirWave's RAPIDS software may be licensed in conjunction with the AirWave Management Platform™ for organizations that manage an authorized wireless LAN or can be licensed on a stand-alone basis by enterprises concerned only with detecting rogue access points.

To arrange a free web demo or onsite evaluation of the RAPIDS software, contact:

airwave

AirWave Wireless Inc.
1700 South El Camino Real
Suite 500
San Mateo, CA 94402

+1.866.802.1121 (toll-free)
+1.650.286.6100

www.airwave.com