AN AIRMAGNET TECHNICAL WHITE PAPER

Best Practices for Rogue Detection and Annihilation

By Lisa Phifer

WWW.AIRMAGNET.COM

Table of Contents

Summary

Rogue wireless devices are an ongoing threat to corporate wireless networks. Network owners need to do more than just scan for unknown devices: they must be able to detect, disable, locate and manage rogue/intruder threats automatically and in real time.

Introduction

Wireless LANs can greatly increase productivity and flexibility by providing anytime-anywhere access to business networks and systems. The same properties that make WLANs so convenient, however, can also leave them vulnerable to misuse and attack by unauthorized or malicious devices.

To safely tap the full potential of WLANs, companies must take steps to find and annihilate these so-called *Rogues*. This paper explains what rogue access points and stations are, why they present a business risk, and how apply industry best practices to effectively:

- detect,
- block,
- locate, and
- eliminate rogues.

A robust plan for managing rogue threats must address all four steps in this critical process, including automated blocking to immediately stop the damage that could occur while your investigation is underway.

Rogue Risks

In an ideal world, the only wireless devices in or near your facility would be known, trusted stations and access points (APs). But, as WLAN adoption grows, that becomes increasingly unlikely. Wireless transmissions from neighboring businesses and homes can easily bleed into your facility, at distances ranging from yards to miles. Furthermore, contractors, customers, suppliers, and other visitors to your facility are more likely than not to carry wireless-capable devices, including laptops, PDAs, and tablet PCs.

In this crowded environment, it can be tough to differentiate between friend and foe. Even the dividing line is not that simple. A new, previously-unknown AP may turn out to belong to a neighbor's network. It may be an unauthorized AP, installed by a well-intentioned but naïve employee. Or it may be a malicious AP, hidden inside your facility for the express purpose of gathering proprietary information. These and several other rogue examples are illustrated in Figure 1.

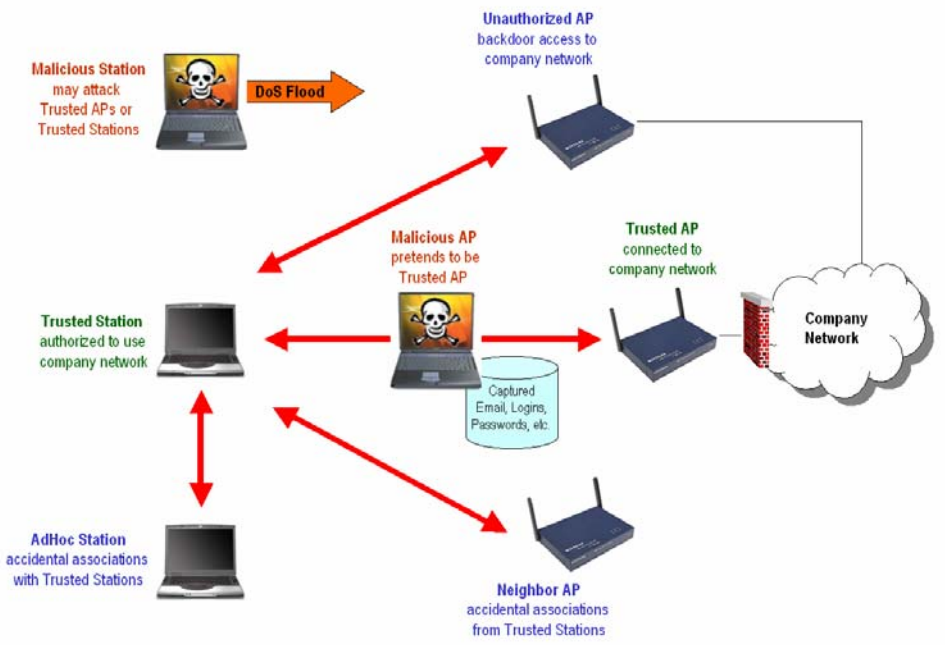

Figure 1: Rogue Devices and Business Risks

In this paper, the term *Rogue* is used to refer to all unauthorized wireless devices, operating within radio proximity, no matter what their intended purpose. For example:

Neighbor APs: 802.11 stations automatically associate with the best available AP, based on criteria like Extended Service Set Identifier (ESSID), received signal strength, and data rates. Some stations can be configured to use specified AP(s), but most cannot -- for example, Windows XP chooses any AP with a given ESSID or any available network. As a result, trusted stations can accidentally associate with APs located upstairs, downstairs, next door, or down the street. Neighbor APs may be benign, but these associations can disrupt private sessions and expose sensitive data.

***Ad Hoc* Associations:** Stations can also connect directly with other stations. These *ad hoc* associations may be used to conveniently share files or send documents to wireless-enabled printers. But peer-to-peer traffic completely bypasses network-enforced security measures like encryption and intrusion prevention. For this reason, many companies ban use of peer-to-peer wireless and should know whenever intentional or accidental *ad hoc* associations occur.

Unauthorized APs: Entry-level APs are readily available, inexpensive, and turn-key. Employees accustomed to wireless convenience at home or on the road often bring unauthorized APs into the office, connecting to the nearest Ethernet. While intentions may be good, the end result is not: an unsecured AP on your trusted LAN is an unlocked backdoor into your network. Guests inside your building and war drivers outside your facility can use unauthorized APs to steal bandwidth, send objectionable content, retrieve confidential data, attack company assets, or use your network to attack others.

Unauthorized Stations: Today, most new laptops and many PDAs ship with factory-installed wireless. Guests who use 802.11 elsewhere may leave adapters active when visiting your office, trying to connect to your APs from lobbies and meeting rooms. Even employees who don't use wireless at work may bring in personal PDAs and PC cards used at home or hotspots. These unauthorized

stations can consume WLAN resources or cause accidental associations, but often draw little attention unless involved an attack.

Malicious Stations: Attacker stations can passively capture traffic, looking for logins, passwords, addresses, server names, and business data. Eavesdropping may be hard to detect, but active attacks are not. Malicious stations can probe or connect to other stations, APs, and WLAN gateways. They can try to redirect traffic using forged ARP or ICMP messages. They can launch Denial of Service (DoS) attacks to block legitimate use -- for example, 802.11 disassociate floods. Malicious stations pose very serious risks and require immediate attention and containment.

Malicious APs: Business risks associated with malicious APs are even greater. Attackers can place an AP inside or near your facility to capture confidential data or modify messages in transit. Tiny hardware APs or laptops running HostAP can easily be concealed within range of many business WLANs. To perform a Man-in-the-Middle attack, the malicious AP uses the same ESSID as your trusted AP. Stations receiving stronger signal from the malicious AP associate with it instead of the trusted AP. The malicious AP can then record, add, delete, or modify frames exchanged between the station and trusted AP.

In short, a rogue device is any unknown or untrusted 802.11 station or AP that warrants further attention to assess and mitigate business risks. Detecting these devices is just the first step to efficiently and effectively defending your WLAN from rogue risks.

Detecting Rogue Devices

New WLAN deployments typically begin with a site survey. WLAN planning tools are used to create a floor plan, specify desired coverage areas, and position APs to deliver service with required capacity and throughput. Portable site survey tools are used to sample received signal strength and noise at defined intervals throughout the coverage area and beyond. Samples are fed back into planning tools, creating actual coverage maps for each AP, ESSID, and channel. Power

outputs are then fine-tuned to avoid gaps or excessive overlap between APs, and channels are assigned to minimize interference.

Rogue discovery plays an important role throughout this process. Before AP installation, potential sources of radio interference must be identified, including walls, doors, microwave ovens, and any existing 802.11 networks. At this stage, you must create a baseline list of untrusted APs and their characteristics, including MAC address, ESSID, channel, signal-to-noise ration (SNR), and approximate location.

It's possible to create this initial rogue list with adapter client utilities or shareware stumblers. But creating a rigorous baseline now will save you time and money later. For efficiency and accuracy, gather data using a professional site survey application, plus a GPS receiver for outdoor surveys. Scan all channels in both 802.11 bands, since rogues may operate any available frequency. Tools that overlay floor maps with AP locations and signal information (see Figure 2) are particularly useful to visualize and understand survey results.

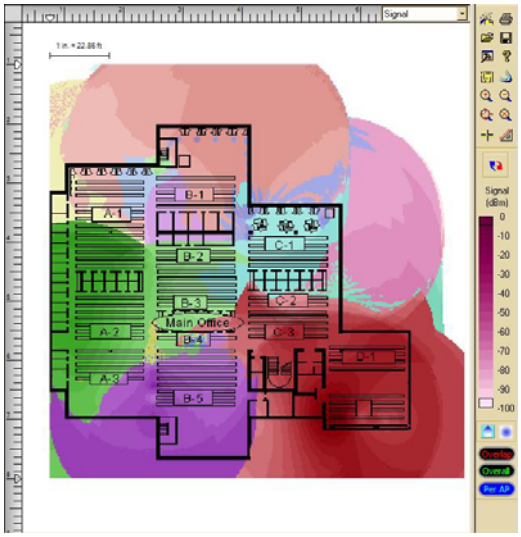

Figure 2: Example Site Survey Output

Site surveys are an iterative process of design, simulation, observation, and adjustment. Once your survey has been completed and your APs have been staged, your baseline list serves as the foundation for on-going rogue surveillance.

As shown in Figure 3, WLANs can be monitored by several complementary systems, including Wireless Intrusion Detection or Prevention Systems (WIDS/WIPS) that offer 24/7 surveillance using distributed sensors to relay observations to a central server, portable WLAN analyzers used for spot-checking and drill-down investigation, and Network Management Systems (NMS) that control AP software, configuration, and operational status.

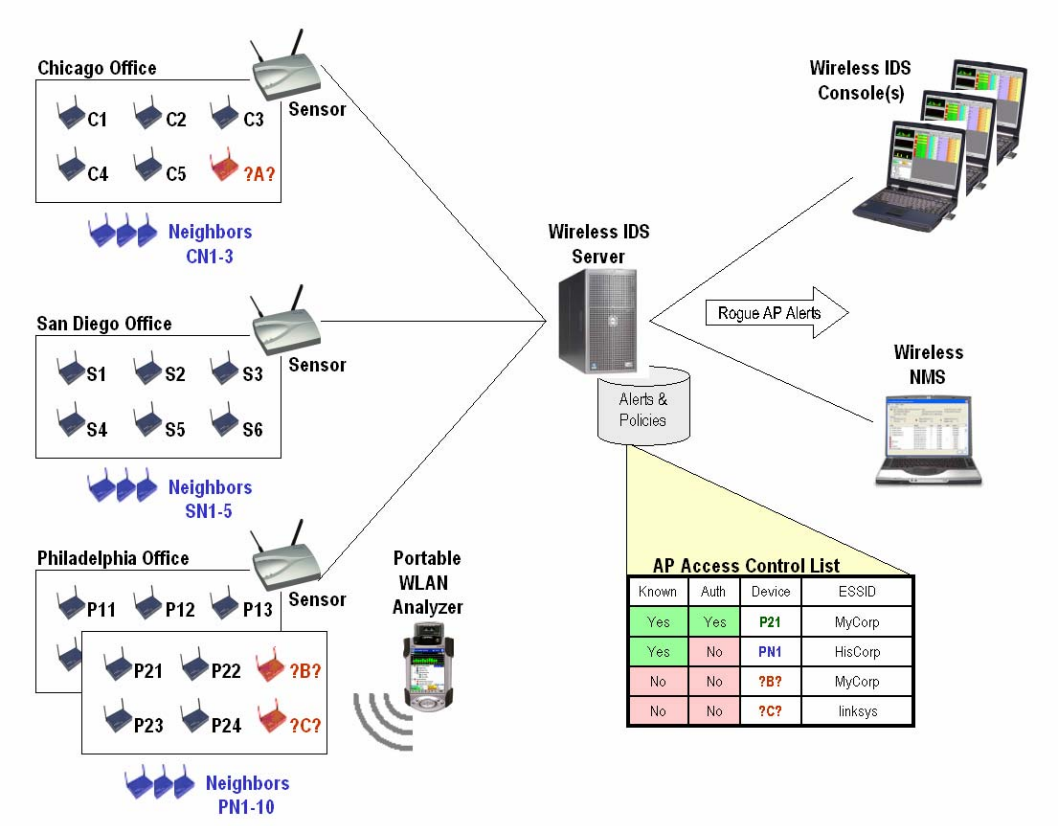

Figure 3: Rogue Surveillance Systems

Each of these systems supports a different set of WLAN management tasks, but all can help you detect suspicious activities that warrant investigation, including rogue devices. To generate Rogue Alerts, these systems rely on Access Control Lists (ACLs) that identify APs and stations by MAC address, a configurable name, and a recently-used IP address. In addition, ACL entries must be configured to differentiate between:

Known/Authorized Devices: APs in your WLAN and stations permitted to use them,

Known/Unauthorized Devices: APs and stations operating in or near your facility that are not part of your WLAN, or

Unknown/Unauthorized Devices: Newly-discovered APs and stations that require investigation and remedial action.

It is safest to assume that each newly-discovered unknown/unauthorized device could be a Malicious AP or Station. For this reason, wireless analyzers and intrusion detection systems typically generate Rogue Alerts upon spotting transmissions from any device not found in the ACL, calling immediate attention to the potential threat.

You don't want to be continuously alerted to the presence of Neighbor APs and Stations, but you *do* want to know if your devices accidentally associate with them. By treating Neighbors as known but unauthorized, Rogue Alerts can focus attention on unknown devices that pose genuine concern, while other alerts can warn of unauthorized activity. For example, you should still be alerted when your authorized stations are communicating with an unauthorized AP, even if it is a known neighbor AP.

In fact, ACLs are just one component of policy: the set of relationships and rules that define secure, robust, correct operation for your WLAN. Depending upon the capabilities of your Wireless Intrusion Detection System, policies can:

- Dictate alert severity, letting you defer action for less important incidents, while calling for rapid response to events with more serious consequences.

- Establish different rules for different devices based on business risk -- for example, ignoring unknown devices using guest SSIDs, but not private SSIDs.

- Escalate alerts based on event frequency -- for example, progressing from alert logging to pager notification to automated blocking as an attack intensifies.

- Forward high-priority alerts to upstream management systems responsible for monitoring the security and health of your entire network.

- Automatically invoke defined actions to disable rogue devices and stop ongoing attacks from causing (further) damage.

Automated policy-based surveillance systems can provide an efficient, effective foundation for rogue management. For ease-of-use and consistency, use integrated systems that can share ACLs and alerts when performing complementary tasks. For example, ACLs created by portable analyzers during site surveys should be exportable to your WIDS and NMS. Alerts generated by your WIDS server should provide easy navigation to remote sensors for incident investigation. WIDS-generated actions that reconfigure devices should be executed through your NMS, letting these supervisory systems do their jobs in tandem.

To ensure that these systems can interact as needed, select survey tools, analyzers, WIDS, and NMS products that are interoperable. You should also beware of rogue detection systems that work with just one brand of AP. Seek solutions that enable effective rogue defense without constraining your network design or equipment purchases.

Neutralizing Rogue Devices

Unauthorized and malicious rogue devices present a real threat, so must be dealt with swiftly to prevent confidential data disclosure, network compromise, damage to vulnerable systems, and other consequences of WLAN misuse or attack.

For example, rogue APs can provide ***immediate*** intruder access to valuable corporate resources. An unsecured AP plugged into an open Ethernet jack can let an outsider reach databases and file servers on the corporate network – bypassing all wireless security that might be provided by properly protected APs. Therefore, network owners must be able to block unauthorized network access immediately, instead of waiting hours or days to physically locate and remove the rogue.

As shown in Figure 4, rogue blocking methods fall into two categories: wired and wireless.

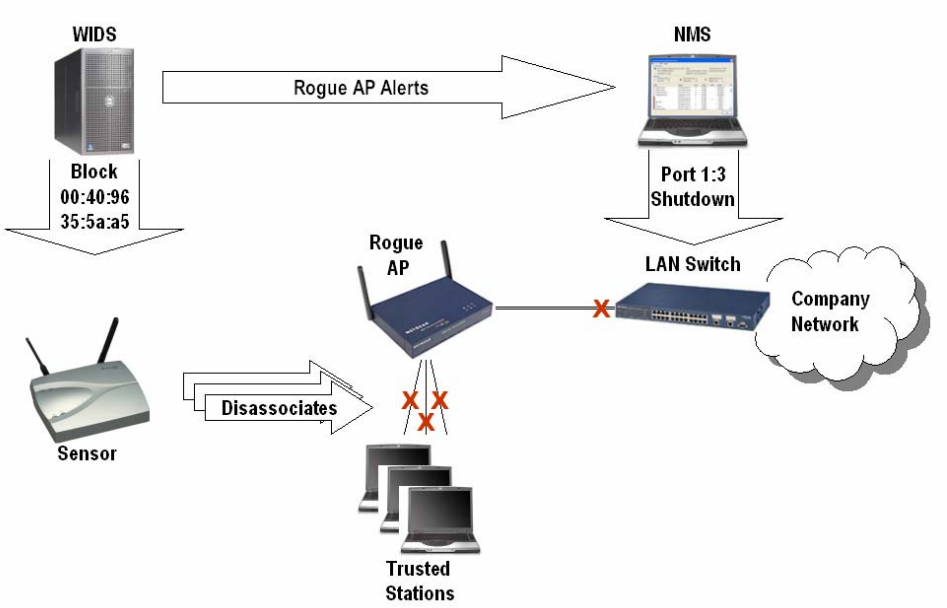

Figure 4: Rogue Blocking Methods

Wired methods prevent a rogue AP (or a rogue station connected to an authorized AP) from penetrating the adjacent network. This can often be accomplished by disabling the LAN switch port closest to the AP's Ethernet point of attachment. Wired-side remedies can also be implemented with firewall or router filters, but blocking LAN access as close to the rogue as possible is most effective.

There are many ways to determine whether a rogue device is on the wired network, and where it is connected. For example, a WIDS can send periodic SNMP or CDP requests to LAN switches to retrieve lists of connected devices, matching those addresses to detected rogues. A WIDS can use traceroute to send wireless traffic to rogues, traversing the wired network to determine a rogue's local subnet and nearest router. Another method is periodic ping-scanning for unknown devices, although this can be inefficient and resource-intensive. In any case, it is essential that you be able to quickly and accurately determine whether a rogue is attached to your wired network.

Once a rogue is located on the wired network, access can be blocked by disabling the LAN switch port closest to the rogue, isolating it from all other wired

resources. An immediate automated blocking action is the best way to protect the wired network from damage, during both short- and long-term intrusions.

Wireless methods prevent a rogue AP (or a rogue station connected to an authorized AP) from productively using the WLAN. This is can be accomplished by repeatedly sending device(s) 802.11 Disassociate or Deauthenticate control frames. These frames can be targeted at a single station or broadcast to all stations using a given AP, effectively preventing new associations or data transmission until the flood ends. Again, the ability to start wireless blocking automatically, at the first sign of intrusion, can be critical to prevent damage while further responses are considered.

Another wireless blocking method is to jam the channel used by a rogue AP or station by generating RF noise at that frequency. This method is far less selective, impacting not just the rogue but any nearby WLAN using that channel. With either method, blocking is usually invoked by a WIDS and carried out by a sensor located near the rogue device.

Wireless rogue blocking methods should be used with great care, and invoked automatically only after extensive experience with manual blocking and risk/benefit analysis. Jamming (and to a lesser extent, flooding) can take down other nearby WLANs, including those owned by neighbors. Clearly, these power tools should be used by trained administrators with authority to take a portion of your network offline. Disabling switch ports may be less disruptive, but can't stop *ad hoc* associations, rogue APs connected to someone else's network, or rogue stations attacking other wireless devices. Ideally, your toolbox should include both wireless and wired blocking methods so that you can apply the technique(s) best suited to each situation.

During a malicious attack, delayed response could let a rogue penetrate further, gather more data, and do more damage. Blocking side effects incurred during incident investigation may be acceptable and justified for short periods, and temporary action may be enough to discourage some war drivers. Surveillance systems that can automate immediate blocking based on very granular policies provide the best foundation for protecting high-value assets.

Locating and Eradicating Rogue Devices

Once a rogue has been detected and (optionally) disabled, you should physically locate the device and decide on a course of action to permanently mitigate on-going risk.

Hunting down a rogue can be time-consuming without proper tools. Wireless devices are often mobile, and wireless associations are by definition transient. If you don't find the rogue quickly, the attacker may move on and you'll never really know what hit you. To narrow your search, start by leveraging location services provided by your WIDS.

A simple but coarse method to predict rogue location uses signal strength to identify the **nearest sensor** (or, in the absence of sensors, the nearest AP or station). The sensor reporting the strongest signal from a rogue is probably within one hundred feet of that device, perhaps less. The rogue may be upstairs, downstairs, or on the same floor as the sensor. In fact, since signal is affected by RF obstructions, attenuation, and reflection, the rogue may actually end up closer to another sensor. Identifying the nearest sensor can provide a starting point, but is usually not accurate enough to conduct a fast, efficient manual search or confidently predict whether the rogue lies inside your facility.

A more complex and more accurate location method involves measuring the rogue's signal strength from three or more points to **triangulate** its probable location. A rogue detected by one sensor can be predicted to lie a certain distance from that sensor, in any direction. A rogue detected by two sensors may be located anywhere those individual predictions intersect. Combining predictions from three sensors can narrow possibilities down to a single location, as shown in Figure 5. Here again, variations in RF behavior affects accuracy, but triangulation with three or more measurements can pinpoint a rogue's location to within 20 feet. This yields a search area that's small enough to readily-determine the affected room(s) and conduct a quick manual search.

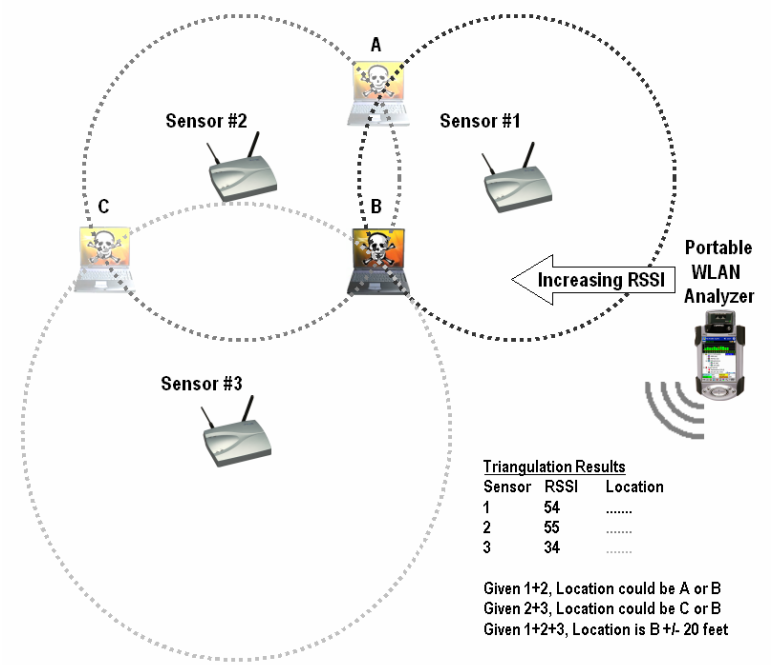

Figure 5: Rogue Location Methods

Your WLAN planning and site survey tools already know the physical layout of your facility and the actual location of sensors, APs, and stations. Your rogue detection solution should leverage that floor plan to **plot the rogue's probable location**, creating a search map.

Ultimately, hunting the rogue down will require on-site staff, armed with a search map. If the rogue is not in plain view (e.g. hidden in a ceiling or cabinet), on-site staff will also need a portable analyzer to listen for rogue transmissions, moving towards the signal source (i.e., in the direction of increasing RSSI). Neighbor and Unauthorized APs may be discovered quickly when using good tools and predictions. Devices that transmit intermittently or move can require a combination of rapid response and patience. For example, triangulation may need to be repeated several times, so look for tools that make this easy by automating both the sampling and plotting process.

In addition, traffic analysis can help you prioritize search efforts by focusing on rogues that present the most immediate danger. Factors to be considered include:

Is the rogue penetrating your wired network? Watch for TCP sessions to inside servers, and use ping or trace to verify wired-side connectivity. For example, use a remote sensor to associate with a rogue AP and aim a traceroute at a server inside your network to identify the wired-side IP address used by the rogue AP. Look for distributed tools that let you easily trace from both sides of the rogue.

How many authorized stations are associated with a rogue AP? An AP that associates only with untrusted stations probably belongs to a neighbor. An AP actively associated with your stations poses a clear privacy risk and could be performing a man-in-the-middle attack. Use monitoring tools that make this kind of ACL-based association information readily available.

What kind of traffic is being generated by a rogue station? A station browsing the Internet may consume bandwidth, but a station generating a DoS flood or port scan is far more likely to be well on its way to doing serious harm. Look for tools that can summarize a rogue's history and present a real-time view of rogue traffic.

The more you know about a rogue's network connectivity and traffic, the better equipped you'll be to take corrective action. Once a rogue has been located, traffic has been analyzed, and threats have been assessed, further action is required to permanently resolve the incident:

If the rogue is determined to be a Neighbor AP or Station, ACL(s) should be updated to avoid triggering future Rogue Alerts. Neighbor APs should be added to your floor plan, including location and ownership details, and channel assignments should be adjusted if needed to avoid interference. Keep an eye on future alerts related to this Neighbor to determine whether additional policy or device adjustments are needed for optimal cohabitation.

If the rogue is found to be an Unauthorized AP or Station, steps must be taken to eliminate the device or (better yet) safeguard and bring it into the fold. For example, Unauthorized APs can be moved outside the firewall, configured with security policies, added to known/authorized AP ACLs, and managed by your NMS. Unauthorized stations can be outfitted with desktop security measures for

safer wireless use outside the office, and their wireless adapters disabled in profiles used at the office.

If a rogue appears to be malicious, carefully review its traffic history to identify all system(s) and data that may have been compromised. To facilitate this, put any suspicious device on a "watch list" to record traffic in greater detail during investigation. To learn an attacker's identity, some organizations even create "honeypots" -- an AP and isolated LAN segment designed to lure rogue stations. If you intend to pursue criminal or civil legal action against a rogue, engage a network forensics expert to guide you through formal evidence gathering procedures. Finally, identify and eliminate vulnerabilities the attacker may have exploited, like compromised logins and passwords used to gain access.

When clearing a Rogue Alert from your surveillance system, create an audit trail of what was done to find, contain, and neutralize the rogue. If you're unable to locate the device on its first visit, history may help nail the rogue on its next visit. Use history reports to spot patterns, identifying holes that should be closed and assessing the speed and effectiveness of your rogue management practices.

How AirMagnet Can Help

AirMagnet provides a strong, comprehensive platform for efficient, effective rogue detection and annihilation. From site surveys and WLAN planning to centralized intrusion detection and on-site response, AirMagnet products can help your organization implement industry best practices for rogue management.

AirMagnet Surveyor supports WLAN planning, simulation, verification, and optimization, delivering results that make it easy to visualize your network and RF behavior in meaningful terms. Surveyor provides a solid foundation for mapping the location of Neighbor, Unauthorized, and Malicious rogue devices, sharing data easily with other AirMagnet products.

AirMagnet Laptop and Handheld Analyzers enable on-site passive and active WLAN observation and analysis. These AirMagnet Mobile Analyzers are the WLAN administrator's Swiss army knives, providing an extensive set of tools to

spot-check network performance, security policy compliance, connection problems, and conduct site surveys. They can record discovered device data and create ACLs for easy import by Surveyor and third-party wireless network managers like AirWave and Wavelink. AirMagnet Mobile Analyzers also provide visual tools to hunt down rogues, associate with them, assess their network connectivity, and identify their wired-side point of attachment.

AirMagnet Enterprise provides robust, scalable 24/7 rogue management, wireless intrusion detection, vulnerability assessment, and policy management and monitoring. **Enterprise** combines central storage, event analysis, and policy-based alert generation with a network of remote sensors that continuously watch for Rogue APs and Stations. **Enterprise** does more than detect rogues -- it incorporates convenient tools to evaluate a rogue's threat level, watch a rogue's traffic, trace a rogue's connectivity from the wired or wireless side, block a rogue from either side, and triangulate the rogue's physical location. Flexible policies and ACLs make it easy to prioritize, escalate, and forward Rogue Alerts to third-party network managers, reducing false alarms associated with neighbors or guests and focusing attention on rogues that pose a significant business risk and warrant immediate, automated response.

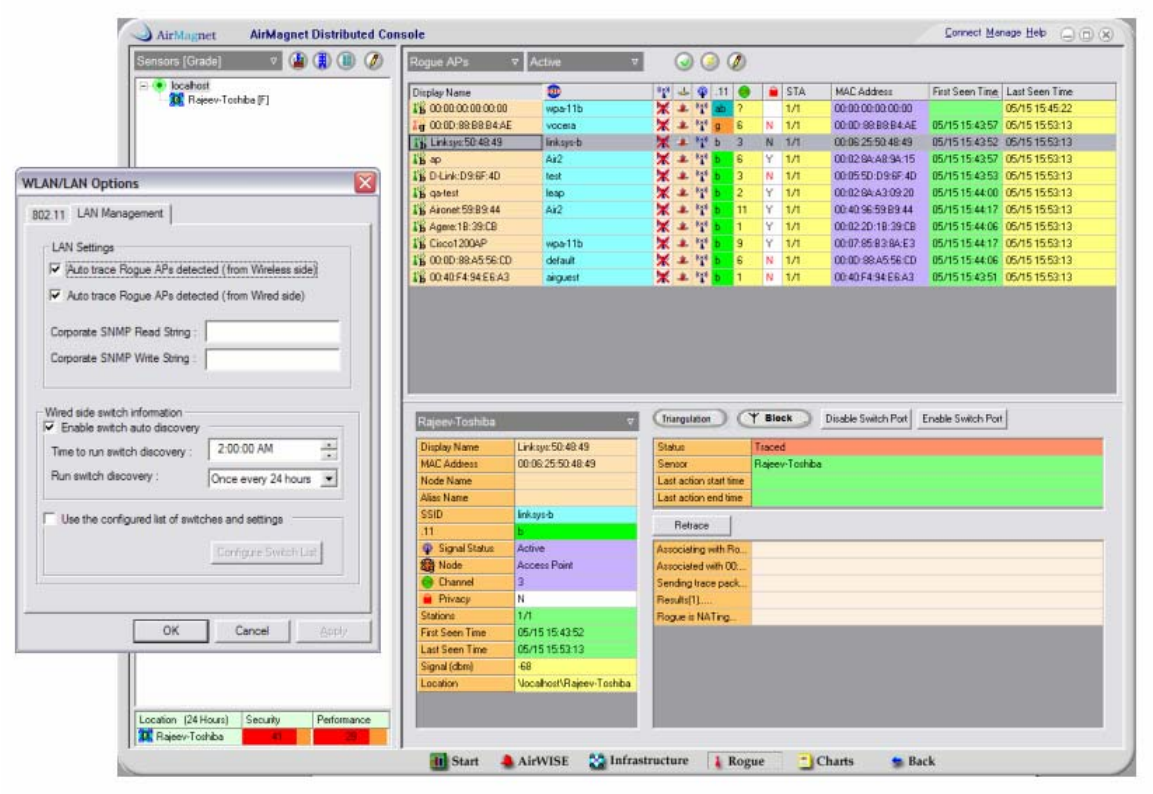

Figure 6: AirMagnet Enterprise Rogue Management Console

About AirMagnet, Inc.

Founded in 2001, AirMagnet, Inc., provides the most trusted WLAN management and security software systems for the enterprise in handheld, laptop and distributed configurations. Used by IT professionals at more than 2,600 companies worldwide in manufacturing, financial, retail, service, health care, utility, transportation, education and government sectors, AirMagnet solves Wi-Fi connection problems, tracks down unauthorized access, simplifies site surveys, and locks in unprecedented levels of network performance, security and reliability. Additional information about AirMagnet and its products is available on the Web at www.AirMagnet.com.