ROGUE ACCESS POINT DETECTION: AUTOMATICALLY DETECT AND MANAGE WIRELESS THREATS TO YOUR NETWORK

The Rogue Access Point Problem

One of the most challenging security concerns for IT managers today is the rogue wireless access point. As 802.11 technologies continue to become more popular, less expensive, and easier for end users to install, the threat to corporate network security increases.

A rogue access point is any Wi-Fi access point connected to your network without authorization. It is not under the management of your network administrators and does not necessarily conform to your network security policies.

A rogue AP allows anyone with a Wi-Fi-equipped device to connect to your corporate network, leaving your IT assets wide open for the casual snooper or criminal hacker.

Rogue APs can be a problem even if your company does not have its own wireless LAN. Often employees seeking to enhance their productivity will innocently install an access point for their personal use on your network without comprehending the security risks.

Consumer-grade vs. Enterprise-class Access Points

Readily available and relatively inexpensive at many popular electronics outlets, consumer-grade access points will easily plug in to your network with user-friendly default configurations and security features turned off. These access points do not identify themselves to you on the network wire (e.g. Linksys, D-Link, Netgear, Belkin, Buffalo, etc.).

In contrast, enterprise-class access points such as Proxim ORiNOCO AP-4000, AP-2000 and AP-600 are designed to be managed. They include management interfaces to the wired side of the network. An enterprise-class AP broadcasts itself to the wired network when it is installed. Wavelink Mobile Manager, a network management and security solution for wireless LANs, can quickly discover an enterprise-class access point and automatically configure it to bring it under management.

Consumer-grade access points are the most common threat to corporate network security. They may be totally silent and transparent to the network administrator. When you try to discover them on the wire, they won't respond. Enterprise-class access points can present a similar threat when their network reporting functions are turned off or disabled, obscuring them from management control.

Proxim highly recommends you establish security policies around the use of wireless access points on your network, and educate your users about the potential threat. At the same time, Proxim recommends putting rogue AP prevention measures into your network to ensure the security of your network.

Common Approaches to Rogue AP Detection

The only way to reliably discover rogue APs is to listen to the airwaves – the wireless side of your network – in combination with the wired side of your network. There are software and hardware products that make the former possible, but on their own they offer incomplete solutions.

Sniffers

One way to find a rogue access point is to search your facility from the wireless side. Sniffer software (such as AirSnort or NetStumbler) allows you to carry a laptop or PDA around your facility scanning all radio frequency (RF) channels for connections with any and all access points within range.

While this software allows you to capture valuable information about the access points in your environment, it can be very time consuming to walk through all of your facilities in search of rogues. And data captured this way is only a sample snapshot – only valid when it is captured.

Further, you must determine whether the unrecognized access points you discover are rogue (within your facility whether connected to your network or not) or simply foreign (operating within range of your airspace, but connected to some other network, i.e. a neighboring business).

While this type of RF audit is often worthwhile, it is costly, incomplete, and too intermittent to continuously protect your wired network from rogues. And if your network covers many geographically dispersed locations, this method of rogue detection may be unworkable.

Probes

To ensure continuous vigilance for rogue APs, you can install full-time probes – electronic devices that continuously monitor all Wi-Fi (802.11) traffic within their range. This can be an expensive proposition. Not just in the cost of the probes (typically $500 to $1000 per device), but also in terms of pulling Ethernet cable and providing electrical power.

However, there is an alternative. If you are already planning to install a Wi-Fi network, dedicated probes aren't necessary. ORiNOCO APs are designed to act as probes as well as Wi-Fi access points, significantly reducing the cost of protecting against rogue APs.

Integrated Rogue AP Detection in ORiNOCO Access Points

ORiNOCO APs are configurable by the network administrator to provide proactive rogue AP detection in both the 2.4 and the 5 GHz band.[1]   Rogue AP detection (RAD) in the ORiNOCO APs is accomplished through low-level 802.11 passive and active scanning functions for effective wireless detection of Access Points in its coverage area. RAD enabled APs service wireless traffic in the foreground while performing RAD scanning in the background thus enabling continuous detection of rogue APs.

While the ORiNOCO APs allow you to aggregate information about all access points operating within range of your wireless network, you still need to determine which of those foreign access points are actually connected to your network wire – and are thus rogue.

To accomplish that, you need a way to know what's operating on both the wireless and the wired side of your network as well as a way to centrally manage and continuously monitor all wireless activity. Wavelink provides that key to the solution.

Managing the Wireless Network Environment

Access point discovery and management is a core capability of Wavelink Mobile Manager. Residing on a server on the wired side of the network, Wavelink Mobile Manager software provides central management control of the wireless elements of the network.

A key capability of Mobile Manager is to monitor the wired network for the introduction of new access points. Mobile Manager discovers new access points by listening at network layers 2 and 3 and by querying switches and routers about the devices connected to them.

Mobile Manager speeds and simplifies the roll-out of wireless technology on a wide-area network by automatically discovering and configuring enterprise-class access points as they are installed at remote locations.

Monitoring the Wireless and the Wired Side of Your Network

After installation, Wavelink Mobile Manager continuously monitors data traffic on both the wireless and the wired sides of a network to provide the most complete approach to detecting rogue access points.

[1] Rogue AP detection is supported in the ORiNOCO AP-4000, AP-2000 and AP-600 Access Points with firmware version 2.4 or higher. The ORiNOCO AP-4000 tri-mode access point and the AP-2000 with both an 802.11b/g and 802.11a radio installed can support scanning of the 2.4 and 5 GHz bands.

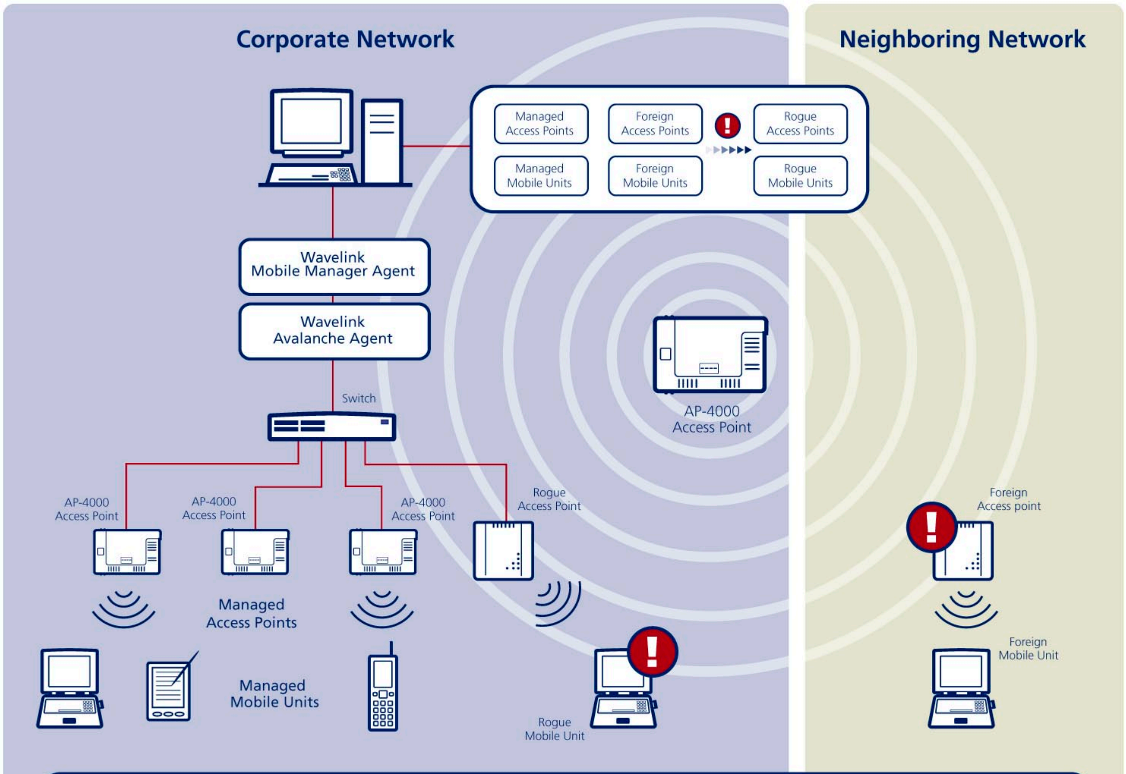
And importantly, Wavelink Mobile Manager allows network administrators to take immediate action to disable rogue APs and prevent intrusion.

Essentially Mobile Manager identifies rogue APs by comparing data from the ORiNOCO APs and/or ORiNOCO clients reporting on the wireless side of a network with what Mobile Manager hears on the wired side. ORiNOCO and Wavelink provide two options for monitoring the wireless airwaves with probes that listen to RF communications in the proximity of your wired network:

1) Integrated rogue AP detection included in ORiNOCO APs
2) Background rogue AP detection in ORiNOCO clients

Using ORiNOCO APs and Wavelink Mobile Manager to Detect Rogue APs and Prevent Intrusion

Access Points discovered in the vicinity of your network may be managed – part of your own wireless network; they may be foreign – part of a neighboring network; or they may be rogue – attached to your network without authorization or management. You can use ORiNOCO Access Points and Wavelink Mobile Manager to identify and categorize all three types of access points and disable the rogues.



Wavelink Mobile Manager compares information it receives from the wireless side of the network with information from the wired side to distinguish between managed APs, foreign APs and rogue APs.

Mobile Manager identifies rogue APs by comparing what it hears on the wired and the wireless sides of the network. First, Mobile Manager generates a list of all mobile devices found by the ORiNOCO APs to be communicating in the wireless environment. Second, Mobile Manager compares that to its own list of all mobile devices known to be communicating through its managed access points.

When the lists are compared, if Mobile Manager finds a wireless mobile device communicating on the wire, but not communicating through a managed access point, then there must be a rogue AP providing access to the wire. Mobile Manager can also identify where that AP is connected to the wire.

To accomplish this, Mobile Manager keeps track of the MAC (Media Access Control) addresses and associated BSSID's of all the mobile devices communicating on the network. Each mobile device carries a Network Interface Card (NIC) with a unique MAC address. The MAC address is incorporated with every packet of information traveling to or from that mobile device.

Mobile Manager also keeps track of where that information enters the wired side of the network. Access Points are ultimately connected to ports on network switches, and these switches maintain a list of the individual MAC addresses of devices communicating through each port on the switch. Using these lists, Mobile Manager can construct its own list of all wireless mobile devices communicating on the wire.

When Mobile Manager detects the MAC address of a mobile device that is not currently associated with one of its managed access points, then that mobile device must be communicating through a rogue access point.

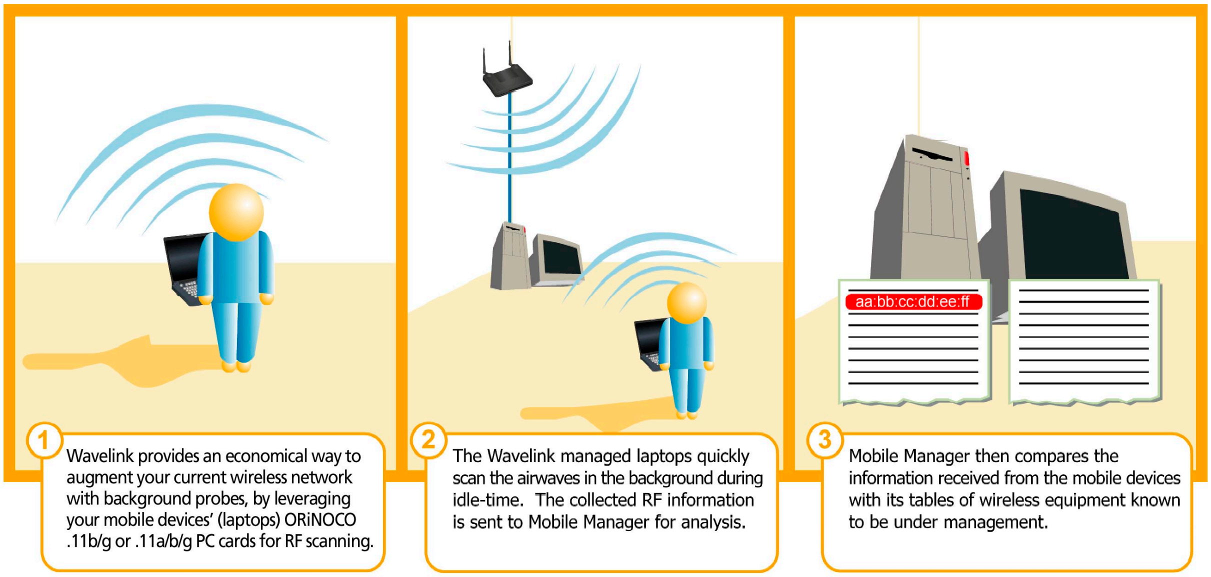
By tracing the individual port and switch where that MAC address appears, Mobile Manager can point to the location of the rogue AP. Network administrators can immediately disable that port, isolating the rogue until it can be physically located and removed, replaced, or properly re-configured according to network security policy.

Augmenting Rogue AP Detection with Background Probes

In addition to scanning for rogue APs through the authorized Wi-Fi infrastructure, ORiNOCO and Wavelink also offer an economical way to augment rogue AP detection with background probes.

At regular intervals and during the course of normal operation, ORiNOCO client cards can quickly scan and record Wi-Fi signals within their range and report back to Mobile Manager. On the wired side of the network, Mobile Manager then compares that information with its tables of wireless equipment known to be under management.

Background Probes: Mobile Devices



1 Wavelink provides an economical way to augment your current wireless network with background probes, by leveraging your mobile devices' (laptops) ORiNOCO .11b/g or .11a/b/g PC cards for RF scanning.

2 The Wavelink managed laptops quickly scan the airwaves in the background during idle-time. The collected RF information is sent to Mobile Manager for analysis.

3 Mobile Manager then compares the information received from the mobile devices with its tables of wireless equipment known to be under management.

While the radios in wireless devices cannot simultaneously communicate data and act as probes, they can be configured to act as probes when they are idle. By enlisting a larger number of mobile devices to listen to the wireless side of your network environment, you have more sources of information to pinpoint rogue APs.

Wavelink Avalanche Enabler can be set to enable the mobile device to act as a probe in idle time, monitoring the airwaves and reporting to Mobile Manager in the background. Wavelink has worked closely with Proxim to enhance wireless network interface cards so they may be used as probes during idle time. In this way, any device using the ORiNOCO 11b/g or 11a/b/g PC Cards[2] and running the Wavelink Avalanche Enabler software can effectively act as a background probe.

Protecting Your Network with ORiNOCO and Wavelink

In summary, to detect and protect against rogue access points, you need a way to monitor the wireless environment as well as the wired side of your network. Consumer grade access points are effectively transparent on the network wire. Even enterprise class access points can be wrongly configured and unmanageable on the wired network.

With ORiNOCO, you can deploy a Wi-Fi network with built-in proactive rogue AP detection, saving costs at the same time as you deploy your Wi-Fi network. Plus ORiNOCO 11b/g and 11a/b/g client cards can be used as background probes to further augment rogue AP detection. Wavelink Mobile Manager delivers central management of all access points and analyzes the data from the APs and background probles to ensure proper configuration and security on your network.

[2] Available on the ORiNOCO 11b/g and 11a/b/g PC Cards using v3.0 software, available June 2004.

Together, ORiNOCO and Wavelink Mobile Manager provide a centralized way to compare what's operating over the air with what's authorized and under management on the wire. More importantly, you can take immediate action to disable a rogue access point as soon as it is discovered, protecting your network security.