



# Enterprise RF Security

Securing wired networks from wireless threats.  
A primer on RF security challenges and solutions.

The simple existence of wireless LAN (WLAN) technology, also known as Wi-Fi, has created a new enterprise security challenge that rivals traditional security threats, including worms, viruses and active intrusion attempts. This threat, unless actively combated, means nothing less than the incontrovertible fact that all wired networks are now inherently insecure in their entirety. We do not intend to over emphasize this particular threat or create undue alarm. We state a simple fact.

Put aside for a minute securing a wireless LAN environment and just think about re-securing wired networks from the real and present threats created solely from the existence of wireless technology. RF security and the ability to “lock the air” is a compelling and urgent imperative to enterprises with or without wireless networks.

#### **All Wired Network Security is Badly Broken**

Wi-Fi is a technology that earned prevalence in consumer markets and is now quickly migrating to the enterprise in an outside-in manner. This evolution is contrary to most enterprise network technologies that originate in the core of corporate or service provider systems and later migrate to branch offices and homes as commoditization occurs. Enterprises not ready to deploy WLAN services have a problem; every knowledge worker in the company can afford, and has the independent capability, to deploy wireless solutions on their own inside the enterprise without the help of IT.

When an enterprise has employees creating their own WLANs, they can never be adequately secured. This, inevitably, results in nothing less than wide-open holes into corporate networks and resources. The enterprise may have policies prohibiting such action on the part of employees, actions that are often entirely innocent in their intent. Yet authorized or not, employees often set up their own WLANs for their own convenience – convenience they have at home and expect at work. The resulting damage is severe.

A more insidious issue is that employees may effectively set up WLAN systems without even knowing it. Microsoft operating systems permit each PC to operate in an “ad hoc” manner – effectively creating a “soft” wireless access point or AP. Consequently, unsecured APs arise spontaneously within an enterprise, entirely without IT control or knowledge. Making matters worse, external intruders may exploit these rogue and soft APs for hostile purpose. This occurs without the knowledge or complicity of the employee who unwittingly enables the attack.

### Holes and Attacks

The vast majority of new laptops are now being shipped with wireless built-in. By the end of 2004, nearly all PCs, laptops and PDAs will be shipped, by default, with 802.11 wireless capability. These capabilities are often used at home where DSL connections are inexpensively extended throughout a house via consumer-grade APs.

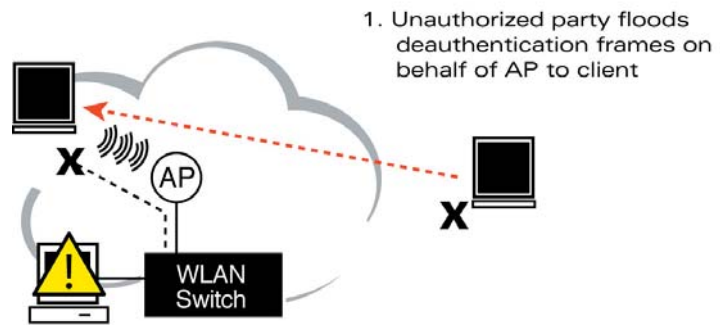
It is quite common for employees to bring these personal APs into work to benefit from the convenience they offer. This is not typically done with hostile intent. Rather, people who are used to the freedom offered by mobility, implement it of their own volition to enhance their own productivity. The problem of using unauthorized APs in an enterprise is known as the “rogue AP” problem.

Most APs are shipped with all security measures turned off. Those security facilities that are available are, at best, weak. For example, the typical encryption protocol shipped with consumer grade APs, called WEP for Wired Equivalency Protocol, has been openly broken. In only a few short minutes, a hacker can gain access to a network via an AP using WEP.

Encryption vulnerability is by no means limited to WEP; even industrial-grade security mechanisms such as the 802.1x framework, that leverages authentication mechanisms, like Cisco Systems Lightweight Extensible Authentication Protocol (LEAP) are vulnerable. Like WEP, LEAP has also been publicly compromised.

Nearly all enterprises have rogue APs deployed without their knowledge. Rogue APs are the easiest security breach to understand but among the most difficult to combat. Yet they are far from unique. The existence of wireless software and technology in general has spawned far more insidious attacks as well. The names and types are endless; monkey jack; honeypot, ESSID jack, Netstumbler, fake AP or station masquerade. Amusing names – devastating consequences.

**Figure 1**  
**Intrusion Detection**  
**and Prevention**  
 Wi-Fi switching to thwart  
 Man-in-the-Middle attacks



1. Unauthorized party floods deauthentication frames on behalf of AP to client

2. Wi-Fi switching system identifies illegal deauthentication frames sent to client from unauthorized third-parties and blocks all future traffic sent from the station so hacker can't obtain proprietary information like NT passwords. Wi-Fi switch then generates alert to administrator.

A PC in a parking lot, for instance, may be used to impersonate a valid corporate AP. A hacker may beacon an ESSID with a legitimate sounding name to entice users to associate with it. This allows immediate access via the victim's PC, while acquiring passwords, control of the PC, local data and an unlimited amount of other data.

How often do such attacks take place? Classes in such attacks are openly taught by hackers and are always sold out. But anecdotes are rendered useless when an RF intrusion detection system is installed. The following are facts:

- It is not wireless networks that render enterprises insecure, it's the mere fact that wireless technology exists.
- Policies without enforcement protect no one. RF hackers depend on such naivety.
- Virtually every large organization has rogue APs active all the time. Their networks are wide open to anyone with the patience to drive around the parking lot until they detect them.
- The combination of Microsoft XP ad hoc wireless networks and Centrino wireless capability enables rogue-like access anywhere, even without rogue APs.
- Exploitation of these RF based attacks is rapidly becoming the fastest growing form of white collar crime. It is not victimless.

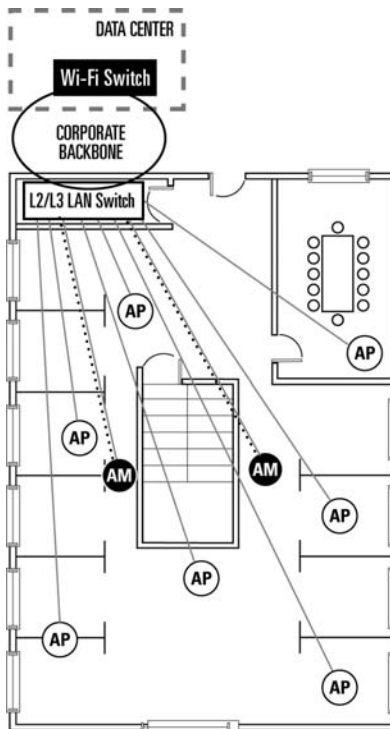
### Intrusion Detection and Prevention

Until recently RF intrusion detection was an oxymoron. It's hard to detect what you can't see or tap and harder still to do something about it. Many organizations have IT staff who walk about their buildings with Pocket PC-based hand sensors searching for (and often finding) rogue APs. This does nothing more than make IT aware of the seriousness of the problem. It is comparable to turning your home alarm on for three minutes per day at random times and never on weekends – the most likely time for rogues to be present and attacks to be underway.

**Figure 2**

#### Centralized Deployment

Dedicated RF air monitors constantly scan the entire RF spectrum looking to detect attacks and unauthorized use of the wireless environment. Once an attack is detected, air monitors actively enforce security policies defined in the Wi-Fi switch.



Aruba Wireless Networks has developed a patent-pending wireless intrusion detection and prevention system (IDPS) based on the same technology it developed to deploy secure wireless capability within the enterprise.

The only necessary ingredients for a successful attack are air, PCs and Ethernet ports. It is the use of air (specifically radio frequencies) that makes wireless intrusion so much more dangerous. To counter this, Aruba makes it possible to literally "lock the air."

This is accomplished by deploying Aruba air monitors throughout each facility. An air monitor is nothing more than an 802.11 a + b/g AP reprogrammed for intrusion detection and prevention.

Air monitors need only be able to hear (receive 802.11 radio transmissions) in each part of a facility. Thus they may be deployed in a much more sparse manner than APs used to provide access to user populations. Air monitors have the important task of detecting, recording, and automatically preventing all RF- based intrusion attacks.

Air monitors are controlled by an Aruba Wi-Fi switch and can be used to provide RF visibility to administrators who have already deployed a wireless network with third-party products. When powered on, each Aruba air monitor boots, determines the location to the nearest Aruba switch and creates a secure, mutually authenticated tunnel (using the standard Generic Routing Encapsulation or GRE protocol) to the Wi-Fi switch.

Using GRE tunnels, air monitors need not be directly connected to a Wi-Fi switch. They may be many router hops away, even on different continents from the Wi-Fi switch. Figure 1 shows how Aruba air monitors might be deployed on a given floor. The Wi-Fi switch, acting as intrusion detection and prevention control center, programs each air monitor to listen for threats. No configuration is required for the air monitors.

Air monitors act as the RF eyes and ears for network managers – giving them sight into all RF activity from a central point and the ability to capture 802.11 packets on demand for immediate traffic analysis. Security and intrusion prevention policies are set in the Aruba Wi-Fi switch and propagated throughout the wireless network.

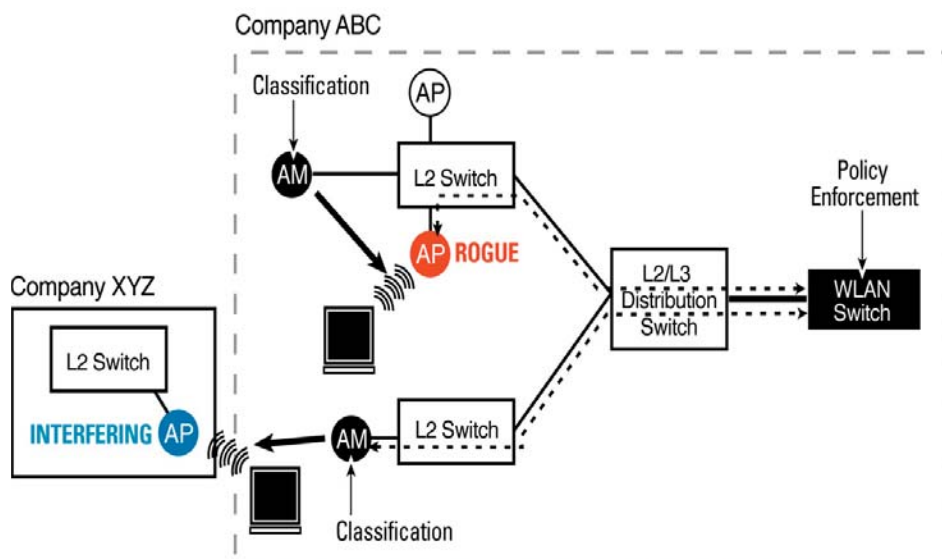
### **Detection, Classification and Destruction**

Listening to all 802.11 radio channels is the basic mechanism used for the detection of all types of RF security faults. In modern WLAN systems, authorized APs are managed actively by Wi-Fi switches and therefore known. To hear an AP or a client in the air is the first step to detection of any of the threats. If unknown wireless activity is heard, a rogue AP, an unauthorized ad hoc (peer to peer wireless) networks, or similar attack may have been discovered.

This process of listening is commonplace among manufacturers of WLAN technology. But it is simply detection of a threat only. Simple detection cannot tell if activity is resultant from a rogue or intrusion attempt or is

**Figure 3****Classification**

Air monitors actively classify all 802.3 traffic seen on the wire and keep lists of valid devices attached to the corporate network. They also monitor 802.11 traffic seen in the air to identify unauthorized activity and proactively enforce security policies defined at the Wi-Fi switch.



simply interfering 802.11 activities from a legitimate neighbor. Second, these systems often use APs for this detection. This is unfortunate since APs cannot effectively listen and transmit on all channels simultaneously. For this reason, Aruba dedicates air monitors to this imperative security function. At any given time, an air monitor can be turned into an AP on the fly to provide for needed capacity on demand while APs can be turned into air monitors in order to quickly troubleshoot a problem or thwart nefarious activity.

Where traditional WLAN technology falls short is in the critical areas of classification and destruction. Is the unknown wireless activity a threat or is it a neighbor? Neighboring AP signals can reach into the corporation causing interference. Wi-Fi switching systems must distinguish between APs that are being used for malicious purposes and interfering APs that can be seen by the user population. User and device classification must be performed automatically without the intervention of humans. Classification must also be 100 percent accurate. No false positives or negatives can be tolerated.

Aruba air monitors and Wi-Fi switches collaborate to provide a complete and accurate classification system. The system uses advanced mechanisms such as comparing MAC addresses and traffic patterns on both the wired and RF environments, coupling this with the sophisticated classification of users and devices.

If RF traffic is unknown and correlated to systems or traffic on the internal network, then one can be certain it is unauthorized, possibly hostile, and certainly not interfering traffic from a nearby home or business. Consequently such users and/or devices are classified as rogue or hostile and destroyed. Destruction comes in the form of disallowing users to associate with a known rogue AP or disallowing unauthorized users from associating with legal APs.

Destruction or prevention of unauthorized RF communications is another unique aspect to Aruba's IDS functionality contained within its RF Lock software. RF Lock, a software module running under Aruba's RF Director management application, uses a number of methods to audit, record, log and then prevent the continuance of the action. At a minimum, the activities existence is recorded (to a syslog) and an alert is automatically generated with important information such as who, where and what was accessed. This action is required for subsequent policy or law enforcement purposes.

Once the attack has been audited, it must be stopped. This may be accomplished on both the wired and wireless sides of the communication. Further, multiple air monitors may use triangulation to pinpoint the location of the offending entities. In short, rogue or intrusion detection without accurate classification is worthless. It amounts to nothing more than informing IT that a problem exists somewhere in the air.

Classification itself is often relegated to a human network manager - an archaic system. Humans make mistakes; RF Lock does not. Classification without subsequent audit and destruction is equally unravelling. Who cares if the alarm company detects a break-in in your home if they do not call the police?

### **RF LOCK: A New Approach to RF Security**

Centralized Wi-Fi switching with advanced RF security is the next step to literally locking the air. Aruba's RF Lock software is a complete RF intrusion detection and prevention system. It detects, classifies, and destroys intruders automatically, while leaving neighboring WLANs in peace. RF Lock addresses the most pressing security problem in wired networks today;

it locks the air. RF Lock provides numerous RF security features to secure enterprise wireless and wired environments.

- o **Wireless Intrusion Detection and Prevention**

Wireless intrusion detection gives the network manager visibility into events ranging from simple probing of the network all the way up to disruptive denial of service attacks or break-in attempts. After detecting an attack or break-in attempt, wireless intrusion prevention kicks in to stop the attacker in his tracks.

- o **Rogue AP Detection and Destruction**

Many products exist on the market to identify rogue APs, but this identification often consists of flagging anything seen over the air as rogue. Aruba's patent-pending classification algorithms allow the system to accurately determine who is a threat and who is not. Once classified, rogue APs are instantly and automatically locked out of the network. Network managers are also notified of the presence of rogue APs, and the approximate location is provided so that they may be physically removed.

- o **AP and Station Impersonation Detection and Protection**

One of the common attacks possible in wireless networks is the "man-in-the-middle" attack, whereby attackers fool the AP or wireless users into allowing the attacker to become a relay point between legitimate nodes. An attacker can use this ability to modify data, corrupt data, or conduct password-cracking routines. Aruba eliminates this vulnerability in two ways. First, Aruba air monitors scan the RF spectrum to detect other wireless stations masquerading as valid APs. If such masquerading is detected, appropriate defense mechanisms are put into place. Second, Aruba Wi-Fi switches keep track of unique "signatures" for each wireless client in the network. If a new station is introduced claiming to be one client, but without the proper signature, a station impersonation attack is detected.

- o **Aruba AP Denial of Service Protection**

Wireless networks by their nature make an attractive and easy target for denial of service attacks. Such attacks include software that floods the network with association requests, attacks that make a laptop look like thousands of APs, and deauthentication floods. Aruba Wi-Fi switches maintain signatures of many different wireless attacks and are able to ignore them so that service is not disrupted.

- o **Honeypot Protection**

With the spread of wireless-friendly operating systems like Windows XP, attackers can make use of “honeypots” - APs placed outside a building that broadcast a legitimate enterprise network ID. Windows XP will generally associate with any configured wireless network it can find - possibly exposing sensitive information to an attacker. Honeypot protection works by monitoring association activity of known wireless clients, and ensuring that they do not stray from the valid enterprise network. In addition, Aruba air monitors will alert the network manager to the presence of a honeypot, and even provide an approximate physical location so that appropriate security staff may be deployed.

- o **Reserves the unlicensed spectrum in multi-tenancy environments**

RF Lock enables policies to be set and enforced based on agreements that you make with your legitimate wireless neighbors. Channels with the 802.11 a/b/g spectrum can be divided up so that interference is reduced. Based on these agreements, RF Lock will implement and enforce that policy, so that friendly neighbors are not classified as a harmful rogue and destroyed.





---

1322 crossman avenue | sunnyvale california 94089

tel 408 227 4500 | fax 408 227 4550

---

[www.arubanetworks.com](http://www.arubanetworks.com)