

Battle for the Wireless Domain: Patents, Issues and Business Solutions

In the battle over patent rights, the USPTO (Patent and Trademark Office) Board of Patent Appeals and Interferences (BPAI) ruled in favor of AirTight Networks and its [U.S. Patent No. 7,002,943](#) in an interference action provoked by competitor, AirDefense. AirDefense provoked the interference by adding new claims to one of its pending patent applications. While AirDefense designed the new claims to look similar to AirTight's already-issued patent claims, the BPAI specifically found AirDefense's application lacked written support for its claims, and therefore "has no standing to challenge the patentability" of AirTight's patent claims. The BPAI entered judgment against AirDefense and in favor of AirTight.

The above clearly illustrate the intensity of the struggle between the leading Wi-Fi IPS vendors to conquer and dominate the wireless markets.

The Stakes

To understand what is at stake, take a look at the projections in the Figure below.

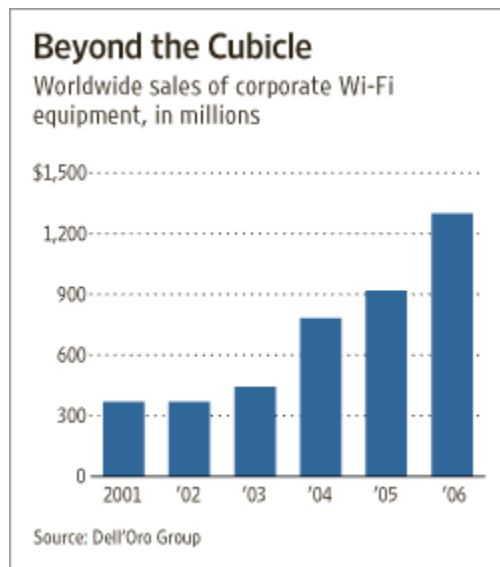


Figure 1: Worldwide sales of corporate Wi-Fi equipment, in millions

According to research firm Dell'Oro Group, the total corporate spending on Wi-Fi equipment is still relatively small, though it's growing – in 2006, companies spent \$1.3 billion on Wi-Fi equipment, up from \$917 million in 2005. In contrast, companies last year spent \$16 billion on equipment that would allow them to access wired corporate networks. **"Clearly there's room for growth, but there are still problems with Wi-Fi that make companies uncomfortable,"** says Elmer Choy, a senior analyst at Dell'Oro.

This re-enforces the fact that demand for wireless protection business solutions will be on the upside and will accelerate when the current difficulties in the implementations and security needs are addressed.

ISSUES

Writing in the Wall Street Journal, Bobby White in an article titled: "Helpless, Hopeless, Wireless" brought to light – in simple language - known real world issues on today's wireless world

"Among the issues is the rising cost of continuously troubleshooting and doing patchwork on corporate wireless network. These have to do with connectivity, loss of connections and signals especially with movements away from the immediate area around a wireless access point (the antenna that receives signals from a wireless device) as users are bounced off the system without warning, while others are unable to make remote connections. Thus, several valuable hours are spent on resolving the issues of corporate networks which uses the wireless technology known as Wi-Fi.

For some employees, the solution to the connectivity issue is piggybacking on a neighboring business's wireless connection that was more stable -- without the other business's consent or knowledge.

Wi-Fi was supposed to reduce complications, not create new ones. The wireless technology was designed to eliminate the cords and cables used to connect computers to the Internet, enabling users to be more mobile and to stay connected to the office even while on the go. Since debuting in the 1990s, the technology has been widely embraced by consumers. Wireless hot spots can now be found at many airports, hotels and Starbucks Corp. coffee shops.

But in many offices, Wi-Fi has been a headache. Like all radio signals, Wi-Fi is subject to interference. Its relatively low power -- less than even a typical cellphone -- means walls and cabinets can significantly reduce signal strength. Wi-Fi also creates a more open network than wired networks, raising security issues.

And Wi-Fi has caused problems for virtual private networks, or VPNs, which are lines of private communication through the public Internet created with encryption software. Some VPNs, which give users access to corporate networks from home or on the road, require a lot of processing power. If a wireless access point -- at home, at the office or on the road -- isn't robust enough, a user often gets bumped off the connection.

Wi-Fi issues have placed a great deal of stress on many corporate IT departments in part because such problems extend beyond the walls of the workplace. Many IT workers are finding that in addition to troubleshooting Wi-Fi problems at the office, they're also called upon to help when colleagues have trouble connecting to their corporate network using Wi-Fi at home, at a hotel or at a remote conference room.

All of this has stunted the growth of Wi-Fi in offices, according to research firm Dell'Oro Group. Some business users have turned away from Wi-Fi entirely.

The difficulties employees have with Wi-Fi at home are often different from the troubles they face at the office. With home users, problems often occur between the configuration of their home connection and the software they have installed to access the corporate network. Sometimes the VPN software isn't compatible with the home network. At work, the main issue is often security, and how to prevent hackers and others from gaining access to the system.

Some wireless networking companies are taking steps to try to deal with customers' problems. One major issue is the stability of the wireless signal. Ruckus Wireless Inc., a wireless networking company based in Sunnyvale, Calif., tries to address that problem by providing wireless access points that have multiple antennas. That allows a Wi-Fi signal to have more than one pathway to an access point -- which can come in handy if something is in the way.

"People want Wi-Fi to do so much more," said Selina Lo, chief executive of Ruckus Wireless. "Small businesses and people at home want it to support things it hadn't in the past."

Alan Cohen, vice president of mobility solutions for Cisco Systems Inc., says Wi-Fi has been hurt in the office environment because the open wireless system creates problems for network administrators who are accustomed to having strict control over a network. With a Wi-Fi network, however, there is less transparency and control, he says. Still, he adds, "this is clearly a growing space."

Some advances in software and hardware have recently eased corporate users' Wi-Fi problems. Companies such as Aruba Networks Inc., AirTight Networks Inc. and Air Defense Inc. have new products that close security holes and alleviate problems with signal strength. AirTight, Mountain View, Calif., for instance, now makes a wireless switch that allows a wireless network to operate like a wired network. That lets IT staffers note attempted attacks on the network and see whether unauthorized devices are attempting to connect in.

Last month, Cisco introduced new software and services that secure and extend the office Wi-Fi network to handheld devices. Some of the new services inspect incoming communications traffic for viruses and block unauthorized users from accessing the wireless network.

Adesa Inc., an auction house in Carmel, Ind., began using Wi-Fi in late 2005. But employees often brought in their own wireless equipment, creating rogue connections to the network and allowing unauthorized users to access confidential information. So last year, Chris Roberts, an Adesa network manager purchased new wireless access points with security software from AirTight; he declined to say how much he paid. After installing the equipment, he found about 173 unauthorized people using the company's wireless network. Those people could have been hackers or people downloading music or movies, which could slow down the network. The new equipment allowed Mr. Roberts to block the unapproved users.

Still, such solutions -- which can cost tens of thousands of dollars -- aren't a panacea. Since Wi-Fi operates on a similar radio frequency as other office or household devices, there tends to be more room for disruption, especially from devices that IT staffers may not originally have thought would be a problem.

That's what happened when doctors with Carilion Health Systems, a Roanoke, Va.-based health company with 100 doctor offices and eight hospitals, began using a new wireless endoscopy capsule last year. When swallowed by a patient, the capsule -- a small device about the size of a vitamin tablet -- wirelessly transmits images to a receiver as it passes through a patient's system.

Carilion's doctors were given a demo capsule early last year, but they hadn't met with the hospital's network administrators to inspect the device before they began testing it. Days later, the capsule's high-powered transmitter ended up disrupting the wireless network for the entire clinic and bumped wireless PCs and handheld scanners used by doctors and nurses off the network. Some of the devices that got knocked off the network held vital records about patients' medication dosages.

"It destroyed communication for some of our devices," says Brian Brindle, senior network engineer at Carilion. The capsule was eventually shut off after network administrators stalked the clinic halls with a Wi-Fi meter capable of detecting unauthorized wireless devices.

Wi-Fi in offices may face further bumps, especially with the growth of new technology like online video. Since video traffic is bulkier than traditional text traffic, watching video over a wireless network can slow access speeds to a crawl and bump users off the network. Last year, a new Wi-Fi standard (there are four others), dubbed 802.11n, debuted and was supposed to solve the problem by improving signal range and download speeds. But upgrading

to the new standard, which requires buying and installing new hardware and software, could prove costly for some.

For Mr. Friemann, Prudential, Fox & Roach's problems continued with the firm's wireless network until he approached managers in October and convinced them that a Wi-Fi overhaul was necessary. In January, the company began upgrading its wireless systems, spending \$120,000 and tapping Aruba Wireless to help. Aruba put in a secure wireless system with high bandwidth access points that allowed the operators to better monitor who was using the network.

Today, Prudential's Wi-Fi network is more stable and Mr. Friemann's time is no longer consumed by troubleshooting. "It used to be when you walked into one of our offices and wanted wireless you had to find someone that knew what they were doing and if not, good luck, you're on your own," he says. "There's still room for improvement but what we have now is definitely better."

The Competition Over Business Solution

The battle over dominance and ownership of wireless IPS business solutions has intensified in recent years. Little wonder that the race to be the first among equals (or unequals) has resulted into false claims and the patent court now deciding on patent origination and ownership.

This is very discomfoting and disturbing as well. And, it does not bode well for an industry that is considered relatively civil. Even with numerous products out there with different labs and organizations benchmarking the products/technologies. Never have their activities wound up in court. Although we all know that each has their pre-conceived notions and in fact for various reasons the products are graded before they are out of incubation.

Among the contenders for market dominance are AirTight networks and AirDefense networks. Both are leaders in their own rights in the marketplace. At stake is rolling out the best business solutions that addresses a wide range of the issues bobby has very well described.

The flagship for Airtight is the **SpectraGuard® Enterprise** - A Comprehensive Wireless IPS and Performance Management Solution.

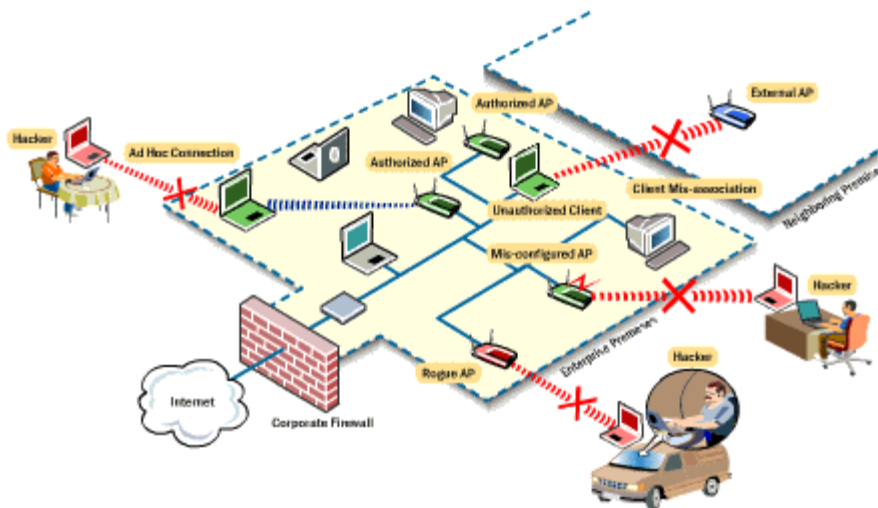


Figure 2: AirTight Deployment

According to AirTight, The SpectraGuard® Enterprise Wireless IPS

- *Automatically prevent all unauthorized Wi-Fi activities*
- Automatically identify and prevent security risks and attacks
- Provide real-time network audits
- Assist in performance troubleshooting
- Monitor the overall health of the wireless LAN

On the other side, AirDefense's flagship is the **Enterprise 7.2™**.

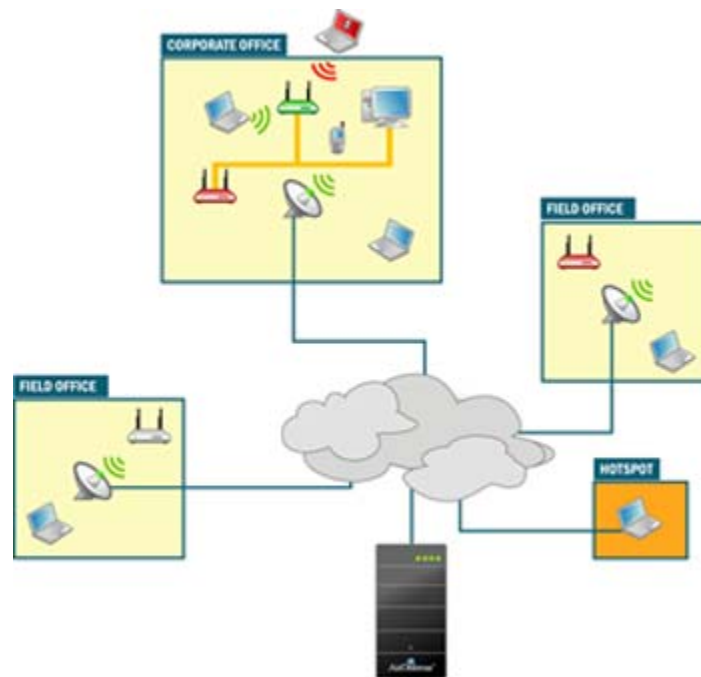


Figure 3: AirDefense Deployment

According to AirDefense the **Enterprise 7.2™** accurately detects and protects the network against all wireless threats and unauthorized devices and provides:

- Comprehensive Intrusion Detection
- Automated Protection
- Eliminate Rogues Connected to the Network
- Comply with Enterprise & Regulatory Policies
- Troubleshoot Wireless Network Performance
- Investigate Incidents with Forensic Data
- Location Tracking
- Enterprise-Class Scalability with Lowest TCO

Hopefully, the claims on the capabilities of the different flagships are true. And if not, then there is a legitimate concern for consumers to pay more attention to the other claims relating to patents, innovations and new products.

As the horizon for wireless networks expands – especially with the fusion of IT with telecommunication - so will the issues, and the rush to churn out the “Best” or “First” business solution(s). In the end, there might be yet more involvements by the patent court in the battle to win the patent war.