

## "Securing the Wireless LAN Installation"



*With an Universal Access Point Enclosure such as this one from Oberon, Inc. most manufacturer's Access Points can be locked and secured in an aesthetic, easy to install, serviceable manner. This enclosure simply drops into the acoustic ceiling tile grid. Aesthetic omni-directional antennas are mounted in the locking door.*

### **Structured Wireless LANS**

Wireless LANs (W-LANs) have become quite popular, providing in-office flexibility and convenience for roaming laptops, voice phones, or other portable devices. This, combined with standardization and aggressive cost reduction, foretells a future enterprise environment wherein the W-LAN prevails as the dominant client connection medium. Commonly, the W-LAN is installed as an overlay to the wired LAN. So, for the network designer and installer, a new opportunity is created to provide the structured wiring to the W-LAN Access Points (the Access Point, or AP, is the data communication equipment which interfaces the wireless client adaptor in the roaming device to the wired network via radio waves). This is a new business opportunity above and beyond traditional network design and installation. However, as popular as the W-LAN equipment has become, there are limitations. Concerns for network security, both the electronic information and the physical components, have become well publicized, and well founded.

The prevailing, standards based W-LAN products are presumably compliant with the Institute for Electrical and Electronic Engineers (IEEE) 802.11b, 802.11a, or 802.11g standards. The standard defines how the radios in the AP and wireless client device will communicate with each other. The standard also describes the basic communication protocol that permits devices to share the common medium - the airwaves. This is similar to the manner in which the IEEE 802.3, or Ethernet, standard describes how devices can

share a twisted pair wire. Products labeled *Wi-Fi compliant* is an indication that the product has been subjected to 802.11b, 802.11a, and 802.11g interoperability tests. Any *Wi-Fi* compliant client device should be interoperable with any other *Wi-Fi* labeled AP or client device.

Given that the network is no longer constrained to components connected by data wires, and that usable radio signal strengths can actually be measured a kilometer away from the access point or wireless client adaptor, how can the wireless network provide reliable coverage where coverage is required, and minimize emissions outside of the coverage area?

The first requirement is for *electronic* security. The standards define, and compliant equipment supports, methods to *authenticate* client adaptors and to *encrypt* the data payload, in order to provide access and information security. Authentication is the process of verifying that the client attempting to engage the network is authorized to do so. Effective encryption will prevent the eavesdropper from using the transmitted information.

The second requirement is to provide *physical* security of the W-LAN components. This involves mounting the access points in such a way that they cannot be stolen, moved, vandalized, blocked, or damaged. It also involves considering RF signal coverage areas, and minimization of coverage outside of the area intended to be covered (one would like to cover the building interior, but perhaps not the parking lot, adjacent buildings, or public hallways). This requires an RF facilities analysis, structured AP placement and wiring, and antenna pattern selection.

## **Electronic Security**

Electronic security is a matter of degrees, and the highest network security generally comes at the highest *initial* cost. But remember, an inadequate security solution could be very costly in terms of network downtime or inadequately protected enterprise communications and information. There are a number of electronic security solutions available for W-LAN, but they may not all be interoperable. Different organizations will have different requirements for electronic security, so it's worth spending the time to understand the target organizations requirements and capabilities. A comprehensive review of security solutions is beyond the scope of this article, but some of the important definitions are provided herein.

The IEEE 802.1x standard describes wire-line authentication, authorization, accounting, and encryption with a layer 2 extension for wireless LANs. This provides a security level on par with most wired networks. 802.1x describes the following:

- Authentication is provided by the Extensible Authentication Protocol (EAP), which occurs between the client and the authentication server. Several different EAP types (EAP-Cisco, EAP-TLS, EAP-TTLS, PEAP) are available, allowing the enterprise to choose the authentication type that best suits its needs.

- Encryption is at the link layer between the W-LAN client and the AP. The current encryption mechanisms available are Wired Equivalent Privacy (WEP) and WEP plus TKIP, Wi-Fi Protected Access (WPA), and Advanced Encryption Standard (AES). The emerging IEEE 802.11i standard for encryption prescribes AES encryption.
- Authorization is controlled by the Virtual LAN (VLAN) membership in combination with the access controls applied at the access router terminating the VLAN.
- Accounting is provided by the RADIUS (Remote Access Dial-up User Service) accounting communicated by the APs to a RADIUS server. Upon authentication, access to the network is controlled by the RADIUS server.

### **Other considerations for Electronic Security**

In addition to the Authentication and Encryption described above, it is generally recommended that the wireless LAN be a separate LAN segment from the wired network. It may also be appropriate to engage a Wireless Intrusion Detection System (W-IDS). The W-IDS is generally comprised of W-IDS sensors distributed throughout the facility, and an IDS server or appliance, which aggregates detected radio packets and is able to report unauthorized APs, unauthorized wireless clients, malicious behavior, and malfunctioning APs and clients. Network security policies should be reviewed, and network managers should periodically audit their facilities for rogue wireless networks or intrusion attempts. The W-IDS can be programmed to enforce these policies. Finally, the APs transmit power should be adjusted to provide RF signal coverage only where desired, and minimize RF signal outside the zone of intended coverage.

### **PHYSICAL SECURITY**

In addition to the electronic security, the network designer and installer should incorporate physical security for the AP. The AP locations are based on the results of an RF site survey or facilities analysis. The site survey is essential for providing effective RF coverage when more than one room is involved, and generally is much more cost effective than guessing AP quantity and location. Because the APs are required to provide RF coverage, they inherently cannot be locked in a telecom facility. The APs, though by their very nature exposed to provide RF coverage, must be protected from theft, accidental moves, vandalism, damage, or blockage. These two requirements are often at odds, so the physical security for the AP must be provided *in-situ*.

Sometimes the AP and its' antennas are placed above the drop ceiling in the plenum space for convenience. However, this is less than ideal for several reasons:

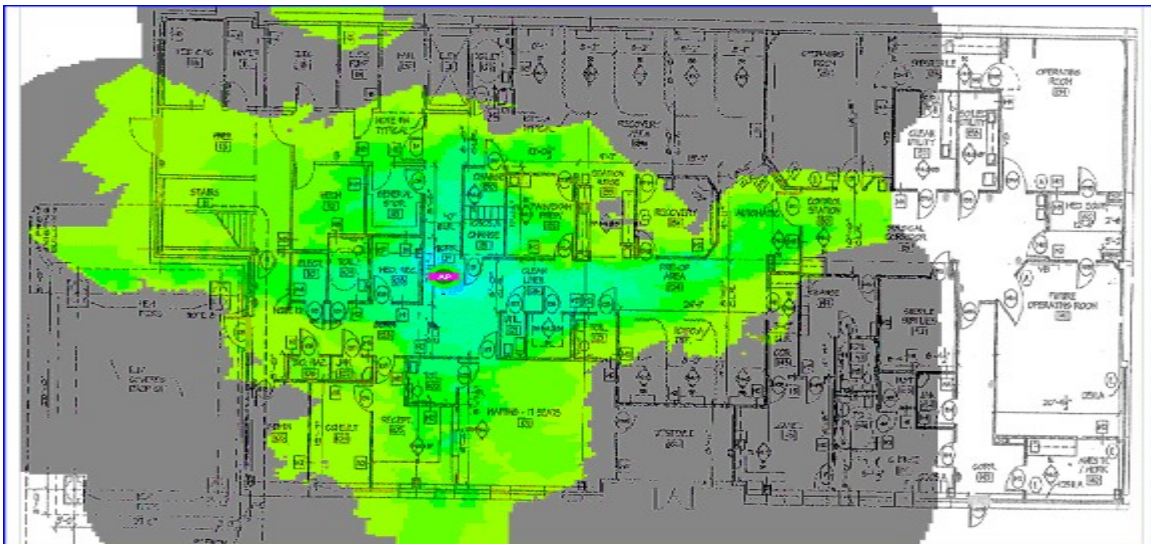
- The drop ceiling may introduce 1-3 dB attenuation between the AP antenna and the area intended to be covered, which results in a 30% reduction in coverage range, and a 50% reduction in coverage area. Because of this, the AP antenna

can be placed in the plenum space only if the RF site survey was performed with the AP antenna in the plenum space. Significantly more APs may be required within the facility to provide desired coverage if the AP's antennas are mounted above the drop ceiling, versus below the drop ceiling.

- Installed in the Plenum space, the AP must be plenum rated and must be installed per national electrical code for plenum space installations.
- Maintenance of the AP may be more difficult within the plenum space, and even locating the AP above the drop ceiling may be a problem.

Ideally, the AP is mounted in an AP enclosure that can be locked and facilitates antenna connection below the drop ceiling. External antennas can be connected to the AP via short coaxial jumper cables, integrated directly with the enclosure, or protrude through the enclosure from the AP. In any case, the antennas used should emulate the antennas used in the RF site survey. The enclosures deter theft, vandalism, and accidental moves, and are less likely to be accidentally blocked. The integrated antennas prevent the antenna from being stolen or tampered with. The enclosures support adds, moves and changes. As AP standards or requirements change, the AP can be swapped out of the enclosure, or additional APs may be added, leaving the data wiring and line wiring in place.

Generally, it is desirable to avoid radiating through plastic or fiberglass enclosures for the reason described above (power attenuation). Also, plastic or fiberglass enclosures may not be acceptable in the plenum space.



*An RF site survey, or facilities analysis, is required to establish correct location and number of APs. This figure shows the RF signal coverage from one AP on a floor of a building. The AP is mounted in an enclosure in the plenum space but the antenna is below the drop ceiling. If the antenna were above the drop ceiling, the coverage could be quite different.*

## Antenna Selection

RF signal coverage can be optimized by using the correct antenna. RF coverage optimization not only means providing RF signal to the wireless client device, but also includes minimizing interference between APs, maximizing data throughput, and minimizing the number of APs used. Most AP manufacturers provide APs with detachable antennas so that the W-LAN designer has flexibility in selection of the antenna type. For APs mounted on the wall, a directional panel antenna, which radiates into the room, is desirable. For APs mounted near the center of the room, an omnidirectional antenna is desirable.

In previous years, the W-LAN designer was constrained to use the AP manufacturer's antenna, and for 802.11a (5GHz band) W-LANs, only APs with non-detachable antennas could be used. The Federal Communications Commission, in July 2004, changed some of its rules regarding use of external antennas with APs. These rule changes give the W-LAN installer more flexibility in their network design for RF signal coverage. According to the rule change (CFR 47, Section 15.204, paragraph (c)(4)), the WLAN designer may use any antenna which is of similar type to the antenna provided by the manufacturer, with equivalent or lower directional gain. 802.11a (5GHz band) APs with detachable antennas are now permitted, so that the W-LAN designer has greater flexibility in using external antennas in an 802.11a W-LAN design.

## Conclusion

Network security is provided in layers. Most importantly, when using the W-LAN equipment, engage the standards based Authentication and Encryption available with Wi-Fi compliant client adaptors and access points (remember, the equipment may be shipped with authentication and encryption "disabled"). Review security policies and isolate the wireless LAN from the wired network. The APs are critical to the W-LANs performance, so it is necessary to physically secure them in order to avoid network downtime and loss of capital equipment. Understand the RF site survey, and install the APs so that they provide optimum RF coverage, while mitigating mutual interference. Select an antenna which is suitable for the area to be covered, and perform the RF site survey with the same type of antenna.

The W-LAN standards are evolving, so anticipate upgrades, either through firmware or hardware, in the near future. Structure the W-LAN design for future performance enhancements, adds, moves, and changes.

*Scott D. Thompson is the President and Founder of Oberon, Inc. He is a Senior Member of the IEEE. He can be contacted at [sdt@oberonwireless.com](mailto:sdt@oberonwireless.com). Oberon's website is [www.oberonwireless.com](http://www.oberonwireless.com). This article appeared in the May 2005 issue of Cabling Installation & Maintenance magazine, PennWell Publishing.*