Table of Contents

I. Introduction .....................................................1
II. Evolution of the Enterprise Wireless LAN Market ..............................................................3
III. Positioning of Intelligence in the Wireless LAN .................................................................4
IV. Enterprise-Class Access Points ....................5
V. Lightweight Access Point Protocol ...............9
VI. Summary ..........................................................10
List of Exhibits

I. Introduction
Drivers for Wireless LANs ........................................................................................................2

IV. Enterprise-Class Access Points
Features for Enterprise-Class Access Point Products ...............................................................5
I. Introduction

The wireless LAN has become more than a niche solution for extending an organization’s wired LAN to difficult-to-wire areas. Supported by a rapidly evolving switching architecture and increasingly robust security, the wireless LAN has entered the IT mainstream. With IT spending limited, wireless LANs help enterprises maintain flexible and reusable local networks: equipment can be re-deployed as an organization changes its locations, workforce numbers, or seeks to enhance employee mobility (see chart, next page).

Enterprises across all vertical industries are realizing operational efficiencies and flexibility benefits in enabling their employees to be mobile while on-site, often creating specific coverage zones within a campus, such as wireless coverage of conference room facilities, or even enabling wireless Internet access for guests within the foyer of a building.

One application that is a key driver for wireless LAN adoption is voice over IP. The creation and deployment of converged WLAN and IP telephony solutions that support voice and data services across enterprise networks are on the horizon; indeed, voice over IP over WLAN is likely to be the application that really drives widespread adoption of WLANs throughout the enterprise.
Additional drivers are highlighted in the following chart from our study *User Plans for Wireless LANs, North America 2003*, for which we interviewed 240 purchase decision-makers from organizations that had wireless LANs as of July 2003 or would have them by July 2004.

**Drivers for Wireless LANs**

- Employees demanding connectivity from common areas such as conference rooms: 70%
- Increasingly mobile employees and addition of office hotels: 69%
- Upgrade/replacement of part of existing LAN: 68%
- Physical changes to sites/new site locations: 63%
- Ability to offer wireless guest access: 53%
- Employees already deploying wireless LANs in their homes: 30%
- Employees already using public WLAN hotspot services: 30%
- Employees deploying rogue access points in your sites or setting up ad-hoc user groups: 17%

Source: *User Plans for Wireless LANs, North America 2003* (Infonetics Research)
II. Evolution of the Enterprise Wireless LAN Market

In 3Q03, enterprises made up 47% of worldwide WLAN hardware revenue, consumers made up 42%, and service providers made up 11%. The enterprise proportion will show the most significant continued increase as enterprise-class switching and security systems drive adoption into this market.

As enterprises continue to build businesses on wireless LANs, vendors have begun to differentiate between SOHO/consumer, small/medium enterprise, large enterprise, and public wireless LAN hotspot products. This has resulted in different grades of WLAN equipment, which is perhaps most evident in the access point (AP). APs are increasingly being designed with different features, performance levels, and pricing to target specific industry segments.

In the enterprise space, the days of building wireless LANs based on cheap SOHO/consumer access points are long over; these devices offer only basic wireless connectivity with rudimentary security and no frills. Though that may be satisfactory in a home network environment, it does not suffice for organizations that need to deploy a network that is easy to manage and control yet is flexible, secure, scalable, reliable, and tightly integrated with the wired network. To achieve these goals, organizations that are serious about their wireless LAN need to look beyond basic functionality and understand the significance of an emerging feature set for access points that delivers the required level of functionality (in other words, access points that are enterprise-class).
III. Positioning of Intelligence in the Wireless LAN

Until recently, the only access points specifically designed for the enterprise were intelligent ones—so-called fat APs, in which all WLAN capabilities are incorporated in the access point itself. This remains a common approach by many enterprise-focused vendors and contrasts significantly with the simple, cheap, basic-function unintelligent access point products that dominate the SOHO/consumer market.

These intelligent access points can be expensive and are awkward for large deployments, as they have few central management functions. These problems have given rise to a new architecture, whereby wireless LAN intelligence is centralized in a WLAN controller and APs have become more lightweight in nature.

It is a misconception that lightweight access points are inherently dumb, providing no more functionality than a SOHO/consumer access point. The lightweight access point has the key defining enterprise-class features and sufficient intelligence to support the performance requirements of an application-rich wireless environment. In addition, when deployed in conjunction with a wireless LAN switch or appliance, it offers the benefits of centralized traffic and channel management, policy, bandwidth, access control, and simple, cost-effective scalability.

Though there remains much debate regarding what functionality should be handled by the switch and what functionality should be handled by the access point, it is clear that there is a need for access points to retain a degree of intelligence and an evolved feature set to be truly enterprise-class.
IV. Enterprise-Class Access Points

As the wireless LAN market matures and vendors increasingly differentiate their products for specific segments of the market, there is an emerging list of key criteria that defines an enterprise-class access point and differentiates it from SOHO/consumer products. In the following chart, from our study *User Plans for Wireless LANs, North America 2003*, respondents rated the importance of features for LAN access point products on a scale of 1 to 7, where 1 means *not important* and 7 means *critical*.

![Chart showing features and their importance for enterprise-class access point products.](chart)

We asked our survey respondents to indicate the features they were looking for in an enterprise access point, but their responses also reflect the features they require in the wireless LAN system as a whole, whether implementing the fat AP model or the aggregation device and thin AP in the lightweight model. In short, this chart reflects user...
perceptions as they become increasingly aware of their organization’s mobility needs and the challenges presented by their existing WLAN architecture.

Based upon the above user feedback, it is Infonetics Research’s belief that the following specific features are required for an access point to be considered enterprise-class:

**Authentication/Encryption:** The threats to wireless LANs are so varied that security is the most highly rated access point feature among enterprises considering wireless LAN adoption. Authentication in particular is a fundamental requirement, as network managers can no longer discern the edge of their network or who is accessing it. Data theft is also a major concern because wireless network encryption—specifically the basic capability of Wired Equivalent Privacy (WEP)—has been highlighted as a weak point. Other threats include attacks that disrupt the wireless service, stealing of bandwidth by external hackers, internal hacking and rogue access points.

Enterprise-class WLAN systems need to have sufficient security capabilities, including layer 3 encryption, such as IPSec, DES (Data Encryption Standard)/3DES (Triple DES), and AES (Advanced Encryption Standard), and other security protocols like Wi-Fi Protected Access (WPA) with the Temporal Key Integrity Protocol (TKIP) and 802.1x with Extensible Authentication Protocol (EAP). While newer WLAN systems provide this functionality in a centralized controller for better configuration and enforcement, emerging standards like 802.11e and 802.11i will most likely require MAC-layer encryption in the AP itself, elevating the AP’s role in overall WLAN security.

**Air Monitoring:** The RF is an open medium that is dynamically changing from one moment to the next. As a result, it is susceptible to real-time threats, such as denial of service (DoS) attacks and the introduction of rogue devices. Real-time air monitoring is therefore an essential feature of a wireless LAN system. For this to occur, access points need the ability to detect unusual activity and react accordingly. In the case of rogue access points, this would include the identification, location, and containment of any unauthorized device.

Many enterprise-class APs will combine air monitoring with traffic delivery to ensure 100% network coverage and to minimize equipment costs. As enterprise wireless networks can grow quite large, this type of integration is an important criterion for an enterprise-class AP.
RF Management: Enterprises need to effectively harness RF and convert it into a reliable and predictable network medium (similar to wireline networks), using statistical data gathered about channel reliability, throughput, interference, applications in use, user location, capacity, and possible network intrusion, to compute the best possible RF topology on the wireless network. With real-time RF management, enterprises can also use the air space to route around WLAN equipment failures, providing fault tolerance and network availability.

While the breadth of RF management capabilities will vary per AP, the following is a minimum subset required by an enterprise-grade product:

- **Dynamic Channel Assignment:** Ease of management becomes a particularly big issue as WLANs grow. Having to manually change the channel settings on an enterprise-wide wireless LAN (with possibly several hundred access points) is not feasible, so enterprise access points need to have standard management information base (MIB) interfaces that can communicate with the rest of the network, including other access points, via SNMP. Even better, many enterprise-grade access points have the ability to dynamically alter their own WLAN configurations to account for changing RF conditions. This eliminates the need to do any ongoing management, remote or otherwise.

- **Adjustable Power Output:** Control over the access point’s power transmit-and-receive sensitivity settings is vital to avoid radio frequency (RF) interference and to balance the network’s coverage and capacity demands; in heavily congested areas, this is vital in RF planning and real-time channel management. The result is a self-configuring, self-optimizing network that delivers fast and reliable performance regardless of network load.

Smart Antennas: Smart antennas improve signal quality, range, and data transfer rates of wireless LAN access points and can improve bandwidth availability and network coverage by using multiple radio signal (called multiple input, multiple output, or MIMO) to electronically steer and/or shape the antenna pattern to more precisely aim it where it is needed; a network with its antennas improperly positioned may have difficulty carrying high resolution video and digital audio reliably, whereas the same network with just a minor change in the antenna position could carry such media rich streams flawlessly.
Scalability and Flexibility: The architecture of the wireless LAN system has a significant impact when an organization looks to rapidly expand its wireless LANs. Adding another access point to a wireless LAN ecosystem that has little centralized intelligence can require reconfiguration of many access points, while adding a lightweight access point to a centrally managed system is straightforward, and arguably more cost effective.

Access points also need to offer flexibility so that they are easily upgradable as the wireless needs of the organization evolve, with dual or even triple radio slots for multiple radio modules so the wireless LAN can be configured to support 802.11a/b, a/g, or b/g users, or even all 3 standards simultaneously. By ensuring that access points can be upgraded to take advantage of new standards for higher speeds as they emerge, enterprises can be more confident of their investment. The enterprise-class access point also requires a flexible mounting system to enable fast and efficient installation in a variety of facilities.

Zero-Touch Operations: Larger WLAN implementations will have a significant number of access points. IT staff cannot be expected to configure and manage APs individually. For cost effective operations, a centralized management architecture is required whereby enterprise-wide policies can be centrally configured and monitored, and pushed out to each access point for local enforcement.

Power over Ethernet: PoE is already widely adopted in the market, particularly in the wireless LAN market, where it can save up to 50% of the overall installation costs by eliminating the need to install separate electrical wiring and power outlets for each access point by delivering power over standard Ethernet cables, which means that network managers only need to run one cable from the wired network to the access point.

Durability: Enterprise-class access points must be housed within a rugged casing to be durable, and must be designed to operate within a broad temperature range and be resistant to humidity for installation in harsh environments such as factories and warehouses, or even outside.

Plenum Ratings: Plenum rating measures an access point’s conformity to the U.S. National Electrical Code UL 2043 specification, one of the regulations designed to reduce fire hazards from electrical equipment in offices, schools, factories, and other buildings. Like all computer or electrical cable, wireless access points installed in the plenum air space should be plenum rated, which means that should the equipment catch
fire it will not emit toxic gases, and this rating is a feature that clearly distinguishes an enterprise-class wireless access point from a consumer product.

**Voice over IP over WLAN (VoWLAN) Capabilities:** As the business case for wireless VoIP gains traction, enterprises will be challenged to manage performance on their local networks to support voice; with great potential cost savings at stake compared to cellular usage in the enterprise, IT managers will have to look to solutions which deliver the necessary QoS functionality as well as load balancing, more efficient traffic distribution and bandwidth management, and low end-to-end latency. VoIP is highly likely to be a key driver in an organization’s decision to implement a wireless LAN, so an enterprise WLAN system, MUST be VoIP-capable, which includes the access points.

**Location-Based Services:** The ability to enforce policies based on the physical location of a user or device provides an additional level of security previously unavailable. Furthermore, location tracking can improve WLAN performance through better capacity planning and enable key enterprise applications such as asset management, enterprise resource planning, and supply chain management. APs assist with location tracking by providing real-time visibility into the RF domain. This can be cross-referenced with known RF characteristics to accurately track user mobility patterns.

### V. Lightweight Access Point Protocol

As most organizations’ wireless LANs organically grow, the ability to manage multiple vendors’ access points becomes more important. Furthermore, as newer generation WLAN systems—which centralize intelligence within a WLAN controller—gain traction, the need exists for interoperability between these devices and different vendors’ access points.

Lightweight Access Point Protocol (LWAPP) is an industry specification proposed to the IETF to address the interoperability issue. It establishes a common set of protocols and procedures governing how lightweight access points can communicate with WLAN controllers.

Widespread adoption of the LWAPP standard will assist enterprises in choosing WLAN equipment that maximizes functionality while reducing the risk of proprietary vendor lock-in. In addition, it would free vendors to focus on innovating features for access points and centralized switches to continue to enhance the capabilities of a truly
enterprise-class wireless LAN system. In this respect, it is essential that an enterprise-class AP comply with a public standard, such as LWAPP, for widespread market adoption.

VI. Summary

The wireless LAN needs of the enterprise market have evolved beyond basic wireless connectivity; organizations are now looking for the same (or better) levels of robustness, reliability, and scalability that they have on the wired LAN and will become more able to distinguish the key features that will deliver their performance criteria.

As the enterprise market has evolved, so has the access point, which has gained an identifiable set of enterprise-class characteristics whilst becoming part of a centrally managed wireless LAN system—also a key requirement expressed by enterprise users.

The access point remains the most significant segment of the WLAN market at this point in time, and has plenty of room for continued innovation and growth. Reports that the enterprise access point segment will rapidly become a commodity have been greatly exaggerated.
About Infonetics Research

Infonetics Research (www.infonetics.com) is an international market research and consulting firm covering the data networking and telecommunications industries in North America, Europe, and Asia. We help companies develop, market, and sell smarter by providing objective analysis of end-users, service providers, and product manufacturers through in-depth research studies, quarterly market share and forecast services, and consulting and custom research services.

We’ve been a leader in the industry since 1990, and the first to peg many new markets, including VPNs, remote access, and ISP networks. We are informed from all sides of the market, and are recognized experts on emerging technologies and markets. We have proven market research methodology and statistical expertise and unrivaled forecast accuracy. Our coverage of buying patterns and user trends is the most in-depth in the industry, and we have a long history of delivering on time, all the time.

Services
- Market share, market size, and forecasts for North America, EMEA, Asia/Pacific, CALA, and worldwide
- Demand-side research on North America and Europe
- Service provider capex for North America, Europe, and Asia/Pacific
- Consulting, retainers, and event speaking
- Custom market research: demand-side research, market size and forecasts, white papers, and competitive analysis

Coverage Areas
- Broadband Networks
- Enterprise Routers and Switches
- Network Downtime
- Next Gen Voice
- Optical and Metro Ethernet
- Service Provider Capex
- Service Provider Routers and Switches
- VPNs and Security
- Wireless LANs

Contact Information

US Headquarters
255 West Julian Street #402
San Jose, CA 95110
United States
t 408.298.7999
f 408.298.2073

Boston Metro Office
3 Baldwin Green Common #307
Woburn, MA 01801
United States
t 781.933.9649
f 781.933.9659

London Office
P.O. Box 629
Bromley, Kent BR1 4WB
United Kingdom
t +44 (0) 20.8290.1954
f +44 (0) 20.8290.1954

For more information or to purchase this study, please contact Larry Howard, Vice President, at larry@infonetics.com, 408.298.7999 x225.