

Public Wireless LAN Market

Wireless LAN (WLAN) saw its beginning in the enterprise in the late 1990s. Early adopter enterprises began deploying the technology in order to solve business problems, streamline processes, and enable the mobility of their workforce within the campus.

During the rapid growth of the Internet, numerous Greenfield service providers emerged that envisioned another potential for WLAN—public access or public WLAN (PWLAN). These providers became known as wireless Internet service providers (WISPs). Their business model was to provide untethered Internet access at public locations by taking advantage of the unlicensed wireless spectrum of 802.11b.

PWLAN Momentum

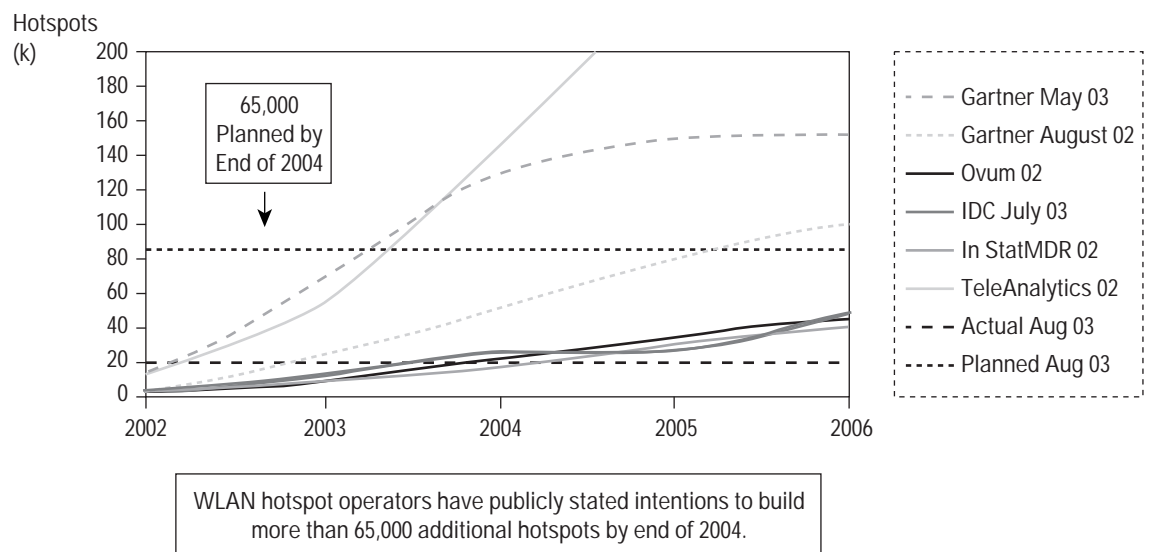
In spite of the poor economic conditions encountered at the beginning of the decade, PWLAN gained momentum, especially among mobile operators that saw PWLAN as a complementary access technology to their existing mobile data networks.

Demand for PWLAN services continues to grow as a result of increased adoption of WLAN technology within the enterprise and home networking markets, and as 802.11-enabled user devices become more common.

PWLAN Outlook

Figure 1 shows the anticipated growth projections being made by various research firms as to the number of hot spots that will be deployed worldwide through the middle of the decade.

Figure 1
 Worldwide Hot-Spot Deployment Actual and Forecasts





The PWLAN market is evolving very quickly. Many service providers have plans for the deployment of PWLAN. Several are moving ahead with their deployment strategies, others are conducting trials with the technology, and a third group is still monitoring the market. Although the analyst projections for PWLAN growth vary, the rate of hot-spot deployments is healthy and is expected to continue climbing.

Seizing the Opportunity

The opportunity to offer PWLAN services is not limited to a particular service provider market segment. Several categories of PWLAN operators are emerging in the market place:

- Mobile operators—Traditional cellular operators, both Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA), are looking at PWLAN as a cost-effective, complementary service to their existing mobile data services.
- Local exchange carriers—These carriers include incumbent LECs, competitive LECs, and international PTTs, many of whom have existing network infrastructure that can be used in the deployment of a PWLAN service. This group is looking to bundle PWLAN services with their other offerings.
- Independent site owners—This type of (non-service provider) operator ranges from airports, hotels, and convention centers to small retail establishments. Site owners typically deploy a PWLAN offering in order to attract patrons to their establishment or enhance the experience they have while visiting an establishment.
- Virtual network operators (VNOs) or WISPs—These carriers represent another category of service provider that either owns its own hot-spot locations or establishes partner relationships with other site owners or providers to offer PWLAN services.
- Cable/Multiple system operators (MSO)—More recently, cable operators are becoming interested in PWLAN as a potential complementary offering to their broadband services. Conversely, other PWLAN operators are interested in partnering with cable operators. By doing so, the PWLAN operator can use the MSO's network to provide WAN connectivity to hot-spot venues served by that MSO.

Hot-Spot Venues

Hot spots are emerging everywhere as operators race to capture venue locations. Examples include:

- Airports
- Hotels
- Convention centers
- Coffee houses
- Fast food restaurants
- Book stores
- Convention centers
- Phone booths
- Airplanes
- And many others...

There is much debate among industry analysts with respect to the viability and profitability of various locations, but most agree that at least today, larger venues—or wherever mobile professionals tend to congregate—represent some of the better opportunities for PWLAN operators.



What PWLAN Operators Should Care About

Simplistically speaking, a PWLAN service can be offered by almost anyone willing to deploy an access point and connect it to the Internet. However, to establish a revenue-generating presence in the market and compete for prime public locations, current and prospective operators must consider the following with respect to deploying a PWLAN service:

Ease of Use

- Easy access—First and foremost, the service needs to be easily accessible so that it is available to the broadest group of subscribers possible. Easy access implies that no special configuration setup or changes are required of one's laptop or mobile computing device.
- Easy sign-up—When a user has access, it must be easy to subscribe to the service. A prospective customer should be able to register and be granted credentials immediately.
- Flexible subscription and payment options—Different mobile users have different access requirements. As such, different subscription offerings such as day-pass, usage-based, and unlimited monthly plans are important in order to attract and retain customers.
- Roaming—A great value comes with being able to roam across hot spots that are owned by a variety of different operators and be billed as if your local operator provided the service. This is very much the way cell phones work today.

Security

- Authentication—Authentication, which includes identifying and validating users before they are granted access to network services, is a mandatory function in a public network in order to control access and collect revenue for services. In PWLAN today, essentially two authentication methods are being deployed:
 - Universal access method (UAM)—This Layer 3 authentication method is common today; it uses a client's Web browser to access the service for the purpose of signing up or submitting credentials in order to log on. Customized client software most often used by VNOs also can perform the same function without user intervention.
 - 802.1x/Extensible Authentication Protocol (EAP)—This Layer 2 authentication technique based upon the 802.1x framework coupled with EAP authentication is not yet widely deployed, but is slowly gaining momentum worldwide. It differs from UAM in that authentication is enforced at the edge of the network through the access point. Several EAP types are available. Because of implementation complexities associated with using certain EAP types in the public space, only a couple, EAP Subscriber Identity Module (EAP-SIM) and Protected EAP (PEAP), are being considered today.
 - EAP-SIM is a method that is just starting to emerge in the industry. It uses SIM-based authentication, which is already a standard method of authentication used by GSM-based mobile operators worldwide. It requires that the client device be equipped with a SIM card and SIM card reader, and a network that is enabled for this capability.

Within both the UAM and EAP frameworks, there exists the ability to use one-time passwords (OTPs) as a method for providing stronger password authentication. Some form of generic token card or soft token program can generate these OTPs, or they could be sent to a subscriber using a mobile operator's Short Message Service (SMS).



- User privacy and protection—To date, certain security compromises exist within PWLAN because of the necessity for broad interoperability between clients and the public network. Specifically, most deployments today do not implement any form of airlink encryption. The industry only recently has begun to address these challenges with emerging standards such as WiFi Protected Access (WPA).

Until there is broad support for the new standards across client platforms, operating systems, and network infrastructure components, PWLAN operators will continue offering “open,” unencrypted access at the access point while at the same time begin offering more secure authentication capabilities.

PWLAN operators need to take advantage of all possible techniques and security measures available “within the network” to mitigate vulnerabilities such as airlink sniffing, IP spoofing, and denial-of-service attacks, all of which are realities associated with “open” access.

Meanwhile, most corporate users will continue to use remote access VPN technology to secure their connections over PWLAN services. This is the same technology used over mobile data services such as General Packet Radio Service (GPRS) or CDMA 1x RTT (Radio Transmission Technology) and usually consists of IP Security (IPSec) or Secure Sockets Layer (SSL).

- Access control and service enablement—This network component or function controls access to services before and after user authentication and authorization occurs. Typical functions include:
 - Captive redirection to Web server portal for subscription to services and service log-on
 - Provide unauthenticated users with free access to specific content often referred to as white list URLs for the purpose of advertising, providing venue-specific information or providing links to subscription servers for service sign-up
 - Accounting record consolidation and generation
- Infrastructure sharing—In order to achieve optimal deployment of 802.11b/g wireless technology, only three no-overlapping channels may be used concurrently. As such, it is often not practical for more than one operator to offer a service at a given location. Many large airports are making it a requirement that only a single PWLAN infrastructure be installed within the facility and the network must be capable of being shared by other service providers. In some cases the network may even need to be shared with nonpublic agencies or enterprises that reside at the airport.
- Location-aware portal branding—It is vitally important for a PWLAN operator to be able to customize what the user sees, depending upon location. This is especially true if an operator is providing access from different venue types. Often an operator will negotiate a revenue-sharing contract with a venue owner that will require that the portal contain co-branded elements.
- Manageability—Effective management of a PWLAN solution is essential for the viability and profitability of this rapidly growing service opportunity. The growth potential of any new provider-operated service is centered not only around its rate of adoption and revenue stream, but also on the cost of deploying the service (capital expenditures [CapEx]) as well as maintaining and supporting its operation and user base (operating expenses [OpEx]). PWLAN is no exception; in order to create a viable service offering, the PWLAN service must be efficiently deployable and effectively manageable.

Network management and operational support methodologies must be considered as part of the service requirements; this ensures the appropriate support metrics are in place to measure the cost of services, return on investment, operational costs, and profit contribution. Functions must be in place to assist with the automation

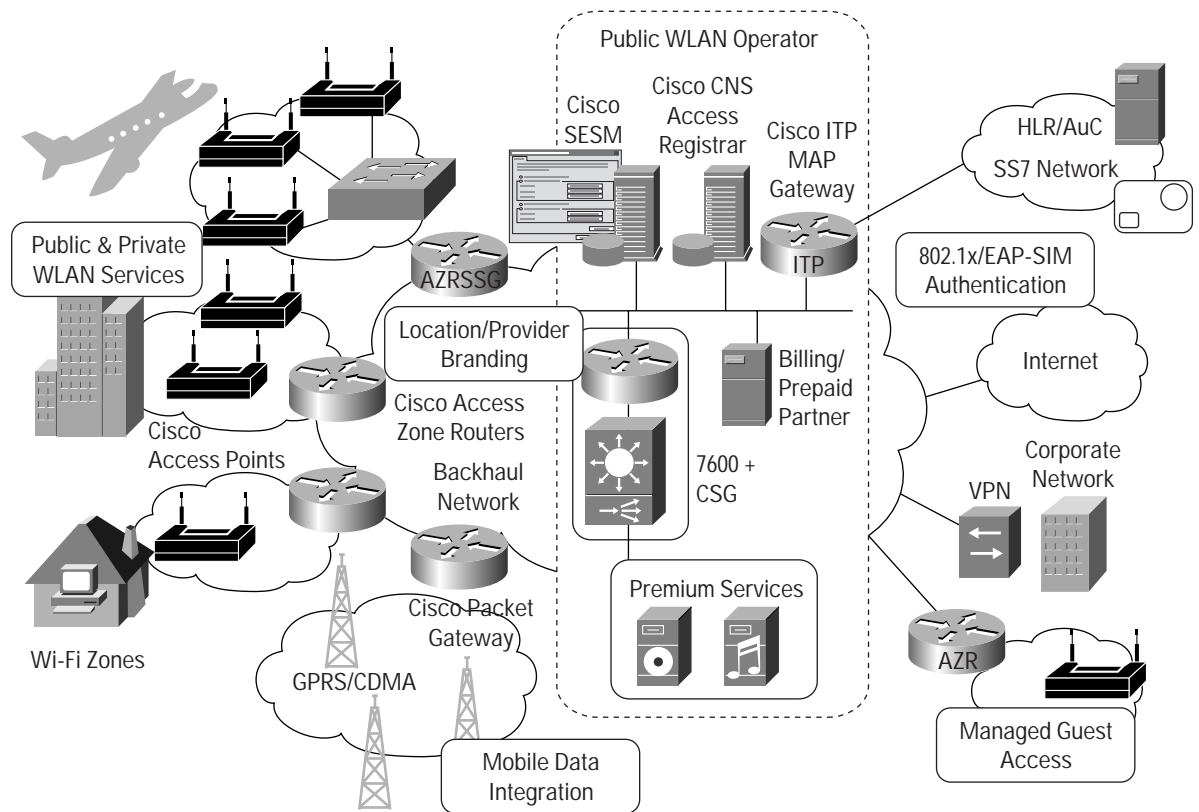


of deploying new service locations, managing and billing increasing numbers of subscribers and subscriber services, tracking and locating faults and service degradation points, and ensuring the stability and security of the system.

The Cisco PWLAN Solution

The Cisco® solution takes advantage of numerous industry-leading Cisco platforms. PWLAN-specific features were developed for these platforms, allowing Cisco Systems® to offer a complete end-to-end solution (Figure 2).

Figure 2
Cisco PWLAN Solution Architecture Overview



Solution Component Overview

- Access points—The Cisco PWLAN solution takes advantage of the highly successful Cisco 1100 Series and Cisco 1200 Series access points.
- Access Zone Router (AZR)—Originally based on the Cisco 1700 platform with solution features now available for Cisco 2600 and Cisco 3700 platforms, the AZR provides connectivity, client address management, security services, and routing across a WAN from each access point to an operator's point of presence (POP) or data center.



- Access control and service enablement—Access control is based on the extremely flexible Cisco IOS Service Selection Gateway (SSG) technology that is now available across a broad range of platforms, including the Cisco 2651XM Router, Cisco 2691 Router, Cisco 3725 Router, Cisco 3745 Router, Cisco 7200 Series, and Cisco 7301 Router. Together with the Cisco CNS Subscriber Edge Services Manager (SESM), the Cisco SSG provides subscriber authentication, service selection, service connection, and accounting capabilities to subscribers of Internet and intranet services.
- Captive portal and branding server—The Cisco CNS SESM works with the Cisco SSG to provide complete control over the subscriber experience, supporting customization and personalization based on device, client, location, service, and other criteria to offer higher value to end users and maximize service and advertising revenue.
- Access Control Server—The Cisco CNS Access Registrar is a RADIUS-compliant, access policy server used to support Web and 802.1x/EAP user authentication. When used in conjunction with the Cisco IP Transfer Point (ITP) MAP gateway, Cisco CNS Access Registrar® performs home location register (HLR) proxy services in support of EAP-SIM authentication for mobile operator networks. Cisco CNS Access Registrar provides carrier-class performance and scalability as well as the extensibility required for integration with evolving service management systems.
- Mobile operator Signaling System 7 (SS7) interconnect—The Cisco ITP is a product for transporting SS7 traffic over IP (SS7oIP) networks. When deployed in a mobile operator's PWLAN network, the Cisco ITP acts as a gateway by taking SIM authentication credentials from 802.1x/EAP-SIM and formatting them into standard SS7 MAP messages for routing to the operator's HLR/AuC. (Authentication Center)
- Network management—Cisco provides a feature-rich element management system combined with a scalable service management layer for robust fault, configuration, and performance capabilities of the PWLAN solution. This includes the CiscoWorks Wireless LAN Solution Engine (WLSE), CiscoWorks LAN Management Solution (LMS), Cisco Distributed Administration Tool (DAT), Cisco Signaling Gateway Manager (SGM), Cisco Information Center (Cisco Info Center), Cisco Networking Services Configuration Engine, and the Cisco CNS Performance Engine (CNS-PE).

Cisco PWLAN Solution Differentiation

Flexibility and Feature Richness

Uniquely positioned to meet today's diverse needs of operators worldwide, the Cisco PWLAN solution provides investment protection for future requirements through continued innovation.

- Shared infrastructure support—The Cisco PWLAN solution can address user group separation and equal access with Layer 2 and Layer 3 methods, thereby allowing providers to offer services for many different scenarios, including outsourced or wholesale PWLAN, guest-access WLAN services, and PWLAN services while using a common infrastructure.
- Services enablement—PWLAN services that offer only a simple gateway to the Internet will quickly become commoditized. Operators need to generate more revenue at lower cost and in shorter timeframes. The Cisco PWLAN solution allows operators to meet this requirement by enabling the introduction of value-added services with incremental revenue streams. Examples of such services include anything from music, movies, sports,



gaming, or ring tones for the consumer, to business-class, WLAN-optimized services for voice over IP (VoIP) for the enterprise or hosted VPN services that offer security for all users. By taking advantage of the richness of Cisco IOS Software, operators can enjoy a unique bundling of solutions to meet emerging requirements.

- Comprehensive branding support—Large customers with prime hot-spot locations such as hotel chains, convention centers, and airports require co-branded, customized portals promoting their business. These portals also must feature localized information such as area guides and points of interest. The Cisco PWLAN solution enables operators to meet these demands. In addition to being able to provide differentiated branding between venue locations or types, the solution can also support differentiated branding within a venue based upon access-point location.
- Flexible service billing options—The Cisco PWLAN solution supports flexible billing models, including postpaid, prepaid (time or volume), tariff, and billing based on subscription content. Additional features enable the network to quickly detect when a user has left the service area without logging out and automatically close their session. In doing so, billing accuracy is preserved and network resources are freed.
- Ready-to-use support for ease of use—Key features developed for the Cisco PWLAN solution allow clients with static host client configurations to access the service without making changes to their laptop or mobile device. Cisco supports clients with static IP and Domain Name System (DNS) entries in addition to supporting clients with static HTTP proxy configurations.
- Authentication transparency—Not all PWLAN subscribers will use UAM (Web based) authentication. As service providers begin to implement emerging 802.1x/EAP authentication methods in their network, there will be scenarios where both authentication methods will exist. The Cisco SSG access control platform can proxy EAP authentication messages from hot-spot access points and automatically create user sessions upon successful EAP authentication, thereby eliminating the need for “double authentication,” first at Layer 2 with 802.1x/EAP and then at Layer 3 through the Web portal. This feature allows an operator to take advantage of the Cisco SSG for centralized accounting record generation for both 802.1x/EAP and Web-authenticated users.
- Open architecture with broad platform feature support—Gives operators the ability to implement centralized, distributed, or hybrid deployment models with flexible platform choices to properly scale their networks.

Carrier Class

The Cisco PWLAN solution today uses carrier-class platforms that are currently deployed in service provider networks throughout the world. Because of the increased emphasis being placed on PWLAN as a “legitimate” broadband service, future phases of the solution will focus on enhancement of the availability metrics of the solution.

Security

It was noted earlier in this document that certain security compromises exist in today’s “open” PWLAN networks. The Cisco PWLAN solution has implemented numerous features in the Cisco IOS Software for Cisco’s access zone routers (AZR) that help mitigate the risk of session hijacking associated with malicious IP spoofing activity.

Operators can take advantage of key features available in Cisco access points to prevent local peer attacks as well as preventing man-in-the-middle spoofing of infrastructure addresses.

Finally, Cisco access points support all 802.1x/EAP methods available today, in addition to supporting WPA for air link encryption.

Summary

The Cisco PWLAN solution embodies all the characteristics and functionality that current and prospective operators need and care about. It is unique in its ability to offer a comprehensive, flexible architecture that enables operators to take advantage of a range of market opportunities today while at the same time creating a foundation for tomorrow's new services.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Cisco IOS are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0304R) ETMG 203253—FK 02.04