May 2003

Spanning the Gap: Products for Public Access Wi-Fi Networks

Q: *Are Home and Enterprise 802.11 networking hardware products appropriate to Public Access Wi-Fi networks?*

Until just the last few years Wireless Fidelity (Wi-Fi) only appealed to the technologically savvy at home, or was one hundred percent implemented and supported by a full time IT staff at work. One promise technology has made for the wireless computing world is ubiquitous Wi-Fi in both private and public spaces, whether for work or leisure. At long last we are starting to see wireless computing really available at your local coffee shack (maybe it's Starbucks™), in your hotel, or in your apartment building. We will see much more! The "Wireless at Home" and "Enterprise Wireless" markets defined the networking products available today. So the question that service providers, who are going to build the Wi-Fi network in your coffee shack and at your hotel, must answer is the one above: "Are Home and Enterprise 802.11 networking hardware products appropriate to Public Access Wi-Fi networks?"

A: No. We need a new class of Wi-Fi access hardware.

The existing wireless solutions that were tailored to fit the Home and Enterprise markets leave unacceptable gaps when tasked with subscriber access in public spaces. These devices are too complex in some areas, too simple in others, and "just not quite right" in yet others. Home and Enterprise Wi-Fi products just do not fit the public, in a literal sense.

The Public Access Opportunity

Subscribers do not have to be sold on the benefits of wireless at this point. "The more the better" will be their motto. Wireless in the coffee shop, in the airport, at the hotel, at the trade show: they want it all. IDC (July 2002) estimates that by 2006, five million subscribers at forty-two thousand locations will regularly access the Internet over public Wi-Fi. Increased demand is driven by the growing number of off-site and mobile workers, currently estimated at seventy-eight million by Cahners In-Stat/MDR and expected to grow to one hundred and six million by 2006. The infrastructure rollout required to support these subscribers will be massive.

A relatively new and exciting technology like public Wi-Fi, with pent-up and growing demand, can get by with less than optimal deployments using whatever hardware is available. However, as consumers get more savvy, service providers begin to butt heads, and investors want more, or any, return on their investments, the spoils of public access will go to the most efficient, best designed network systems. Will these new public access networks just be extensions of the well known Home and Enterprise networks? Or something new? Wireless network architects can make three design determinations, we would hope based on their analysis of user's needs.

- Are Public Users Like Small Office/Home Office (SOHO) Users?

  This design presumes that the first concern of public access systems is cost. SOHO hardware is ultra-cheap and designed to be easy to deploy. Though generic and inflexible, these gateways have hit a fifty-dollar price point, or even less in bulk. You get what you pay for, of course.

- Are Public Users Like Enterprise Users?

  This design presumes that the primary concerns of public access Wi-Fi users are security and performance. Enterprise hardware is the best of the best wireless technology has to offer. High performance, high gain (signal strength, range, and quality), high security. Cost is one big disadvantage, with enterprise gateways and access points in the four hundred to eight hundred dollar range. The biggest question for enterprise hardware is whether the features you are paying for in an enterprise box are valuable to public access users, and are there other features that enterprise users did not even want that are public access 'must haves'.

- Do Public Users Have Unique Requirements?

  This design makes network architects nervous. Few people like dealing with new scenarios that defy convenient pigeon holing. The presumption here is that public access Wi-Fi users have different requirements than existing customers in the home and office. Rather than trying to match the existing hardware to these users, the system is designed from the ground up to address the exact public access requirements. The disadvantage here is that there may be few, or no, manufacturers with the 'just right' gateway for public access.

How to Deploy a Public Wi-Fi Network

Before the network architect can decide what kind of hardware to deploy, an assessment of the system's requirements must be made. In addition to those features the end user/subscriber wants and will pay for, consideration must be made of the software applications used for billing and configuration by the Wireless Internet Service Provider (WISP), as well as the requirements of IT professionals who must manage the system. The hardware itself might be a wireless LAN access point connected to a hard wired WAN gateway, or a combination wireless WAN and LAN gateway.

A Simple Public Wi-Fi Use Case:

An example of how we think a user will approach and use the service will inform a discussion of requirements. Joe and Jane are business travelers with laptops configured with static IP addresses, email configuration, and http proxies. Joe is a direct T-Mobile subscriber, while Jane uses Boingo through their partner network. When traveling they need email and web browsing and they may even want to print locally. All this needs to work quickly and easily, without adding or changing any settings on their laptops.

Public Wi-Fi hardware requirements:

1. Network connectivity so users can access the Internet, browse, email, etc.

   As the no-brainer, the hardware must have basic network support along with all that entails. Any gateway, home, enterprise or other would be expected to have these technologies, among others:

   802.11b or 802.11g, IP Routing (TCP/UDP, ARP, ICMP), NAT and NATP, DHCP, DNS, PPP

2. Configurability

   The plethora of possible venues where these devices may be found means that the gateway itself must be manageable and configurable in many different ways. A basic HTML management interface will satisfy a small venue, while more sophisticated networks require a telnet-based Command Line Interface (CLI) or the Simple Network Management Protocol (SNMP). In addition, a sophisticated provider may have an

XML-based Operations Support System (OSS) used to automatically configure and monitor the network, requiring the gateway to support a web services model based on the Simple Object Access Protocol (SOAP).

3.   Security

Privacy and protection against theft of service are the top concerns for users and providers respectively. Joe and Jane do not want anyone reading their private emails. T-Mobile, Boingo, and the Coffee Shack do not want hackers using the network for free, especially if they are not even drinking any cappuccino. Security has to work for everybody involved.

a.   802.1x to address well-known WEP weaknesses

Unfortunately, a minimally skilled hacker can get free software to crack a WEP system and get full access within days or hours, depending on the volume of activity. A large public network, like an airport, would be extremely vulnerable. Longer or shorter encryption keys do not help this weakness. The new 802.1x enhancement to WEP protects the encryption keys using RADIUS to change them frequently. Supporting 802.1x require RADIUS support as well.

b.   Secure Web browsing using HTTPS

Hyper Text Transport Protocol: Secure (HTTPS) using Secure Socket Layer (SSL) or Transport Layer Security (TLS) is the Internet standard for browser privacy via encryption. One possible complication is that the hardware itself must have its own HTTPS system. Configuration by an operator using the device's HTML GUI and users logging onto the system using their private name and password must be protected as well. Some gateways may only pass-through HTTPS from user machines the Internet, and may not have their own encrypted HTTP Server. This leaves unacceptable security vulnerability in the gateway.

c.   VPN pass through

Virtual Private Networks (VPNs) are a way to create a private connection between machines that provides greatly improved security. Most likely Joe and Jane will log onto a VPN provided by their company, and set up by their IT staff, if they want to access company machines from outside the corporate network. It is important that a gateway support this kind of VPN. An additional VPN feature is the ability to terminate, rather than pass through, a VPN connection, meaning that the VPN connection starts or stops at the gateway itself. This is a key feature of an enterprise access point, but in general public users will want to connect to their existing company VPN, not create a new one at the airport.

d.   Firewall

A firewall is a standard piece to software that would be in any but the lowest end gateway. It is very important to protect the network from malicious packets, worms, denial of service, and the like.

e.   "Blacklist" to ban abusive subscribers

The gateway must allow the operator to identify bad actors on the network and prevent them from logging on again. Just canceling their account is not sufficient, since malicious users may just log on again under another name. A blacklist can associate these users with the MAC Address of their network card, preventing them from just logging on again with a new account.

4.   RADIUS Billing Support

Authentication, Access and Accounting (AAA) for Wireless ISP subscribers is generally accomplished using the well-defined Remote Authentication Dial In User Service (RADIUS) standard. This standard was originally designed for user access to modem banks, but has proven up to the task for wireless access control today. The WISP uses RADIUS to insure users are legitimate, track their usage patterns, bill value-added services, and any number of other account management chores. In addition, 802.1x depends

on RADIUS to protect the encryption keys. This makes RADIUS support extremely important for wireless access hardware.

    a.   Local RADIUS

One limitation of RADIUS is that it generally requires a separate RADIUS Server that is dedicated to tracking subscribers. Mostly often this server resides at a central location, such as the WISP headquarters. The problem is twofold. First, small venues may not have a central authority, leaving them to try to deal with installing an esoteric RADIUS server. Second, a network dependent on RADIUS for 802.1x security becomes vulnerable, or totally unusable, if the connection to the RADIUS authority is lost. For these two reasons a local RADIUS server, either on the gateway itself or as a separate device, is necessary.

    b.   Local Credit Card Authentication

A typical business model for public Wi-Fi is for users to log onto the network and then provide a credit card for daily or hourly access. Since AAA services are not coming from a central RADIUS server in a local configuration, the gateway must provide credit card authentication as well.

5.   Multiple WISP Support

A wireless network is beholden to a single WISP unless the gateway is capable of supporting several groups of subscribers simultaneously. Jane and Joe need to log onto different service home pages with different RADIUS Servers and different terms of service to get access to their T-Mobile and Boingo connections. The network hardware should be capable of supporting different user groups based on their preferred provider and subsequently distinguish between them. One way to create different user groups is by using multiple SSIDs at the access point.

6.   WISP Branding

Given that multiple WISPs are accessible on a particular public network, those providers will insist on being able to present their interfaces in accordance with their corporate image, with customized login pages, web content, etc. The access hardware must keep track of these ISP-provided brandings based on user selection of ISP. In addition, each WISP has separate Walled Gardens (pre-approved web pages not requiring log on) that their subscribers, actual or prospective, can access.

7.   Physical Deployment

The sheer variety of possible public venues means the hardware must be available with and without secure enclosures (so you can not steal it off the wall in the airport lounge), and with different antenna options offering different signal strength and direction. Some venues may even need weatherproof outdoor enclosures.

8.   Transparency

Transparency is a catch all for the user experience of "everything just working". Because Jane and Joe, or any typical user, cannot be required to reconfigure their laptop, the network must support their laptops as they are. This extends to not installing proprietary clients, printer drivers, or any other software.

    a.   Printing

Typically wireless printing is just an extension of regular printing over the LAN. However, the user needs the appropriate printer driver installed. Since there is no guarantee that a user in the hotel will have a particular driver, the network must support a more generic method of printing to a local printer in the hotel lobby, airport information kiosk, or attached directly to the gateway itself. This could be accomplished using a file upload to a web page on the gateway, or via an email attachment.

b. IP Settings

User laptops may have any combination of static and dynamic IP settings, HTTP proxies, or other network settings. Realistically, these can not be changed each the time the user wants to connect, so the network must be configured to support any possible setting silently and transparently.

c. Email

As with IP settings above, public users may have any combination of Simple Mail Transport Protocol (SMTP) settings. In particular, subscribers may be using a SMTP server to send their email where SMTP does not accept email from outside a private network. Without intervention the subscriber's SMTP server will not send these emails. The network must insure that this email is correctly delivered by using its own SMTP server.

d. WISP

As in 5 and 5a above, the user must be able to select their specific WISP, assuming it is supported by the network, with branding, login methodology, and all of the other features that the subscriber is accustomed to from their WISP.

A typical public access Wi-Fi application looks like the diagram below. Please note that the gateway is often authenticating to more than one Network Operating Center, so that different service providers may be supported at the location. In addition, 802.1x/RADIUS server functionality may be in the gateway itself for local authentication. The bottom line is that the gateway needs to be flexible enough to support different usage and billing scenarios.
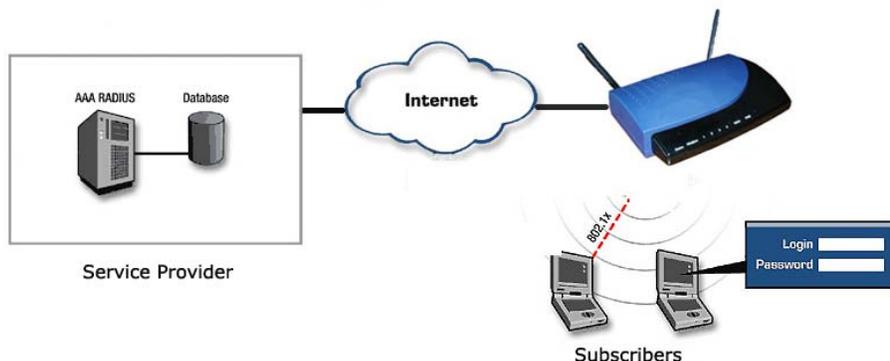
Home (SOHO) Wi-Fi: Too Cold

At fifty dollars, or less, the price is right for SOHO gateways and access points. But how do they measure up to our requirements for a successful public network? Looking at the requirements above, not very well. The only area where SOHO hardware measures up is basic connectivity and a firewall. Configurability is in most cases limited to a Web GUI only, security consists of the vulnerable WEP, and RADIUS is absent in any form. No RADIUS means no WISP support at all, and a SOHO gateway is not going to handle any kind of non-standard user settings of any kind.

Conclusion

Even at such a low price point, a Home Gateway is just not feature rich enough to be usable in a public network that has any kind of billing or security requirements. The money saved in deployment would just be squandered as users and operators became frustrated with the configuration problems and lack of features. This kind of gateway might be appropriate for a totally free "hotspot" in a café where it was free and open to all.

Enterprise Wi-Fi: Too Hot

At four hundred to eight hundred dollars, or more, the Enterprise gateway is a fine piece of hardware. Basic connectivity is there of course, and probably includes 802.11a, with its greater access speed, as well. Configurability via Web and SNMP are definite, with CLI probably, and SOAP maybe. Security is excellent, and probably includes VPN termination, and possibly a proprietary WLAN client with improved security (Cisco LEAP for example). RADIUS support is there, but probably not local RADIUS except at the top end. Firewall and deployment options are definitely there. However, there are some important features missing as well that may make the Enterprise gateway seem a little tepid. Multi-WISP support and WISP branding are not needed nor included in an Enterprise gateway. The transparency requirements are just not Enterprise issues, because the IT department can control the user's laptop settings. So Email, printing, and IP configuration are just going to be unavoidable headaches for users. The user can resolve email and IP configuration problems by reconfiguring their laptop, which will work for technology savvy subscribers, but printing just will not work.

Conclusion

It must be recognized that the public Wi-Fi networks and "hotspots" that we enjoy today are for the most part based on deployment of Enterprise gateways, so there must have something going for them. The question, then, is Enterprise hardware the right answer? Creating a public network using enterprise gateways and access points is a waste of excellent technology and money. The extra features like VPN termination and 802.11a are simply not appropriate. Even worse, only the highest-end devices are likely to have local RADIUS, multiple WISP support, and SOAP, making this a painfully hot solution indeed. Billing and branding are the keys to successful public access Wi-Fi deployment. These issues are completely irrelevant to the Enterprise.

Public Access Wi-Fi: Just Right

A public access Wi-Fi gateway specially designed to satisfy our public access requirements will, of course, be right on target. On target to the extent that we have understood our customers. The danger was that no one would step forward to address these requirements, leaving no option for service providers wishing to establish a serious and profitable business for public access Wi-Fi. Fortunately, a select group of new companies, including ValuePoint Networks, are already moving ahead in this market space. These companies are providing products that fall into a spectrum of prices that match the requirements for a Public Access Wi-Fi deployment.

Conclusion

Superior branding and billing services are to key to the success of anyone deploying a network for public access Wi-Fi. Security and new feature technologies will become commodities once the excitement fades. Subscriber loyalty will be based on ease of use, as it always is. Given the plethora of Wi-Fi hardware available for Home and Enterprise, when architecting your public access Wi-Fi network choose hardware "purpose built" to contribute to your ultimate success.   Design your network for all of the parties involved. Choose products designed from the ground up for **billing, branding,** and **transparency** in a public Wi-Fi network.