



**RSM Experts**

Knowledge & Skill  
at your service.



## **Understanding the WiFi hotspot business**

An introduction to the concepts, markets, challenges and technology



**The Standard for  
Wireless Fidelity.**

A  
RSM Experts  
White Paper  
<http://www.rsmexperts.com>

**Author:** Daniel Koffler  
**Date Released:** Jan. 2004  
**Last Revision:** June 2004

## **Understanding the wireless hotspot business**

This document is meant to serve as a business oriented guide that will introduce the concepts, markets, challenges, processes and technology required to implement a successful public WiFi hotspot or hotspot network.

This is not a technical guide, though it does discuss the assorted equipment required. Whether you are interested in setting up a hotspot at your location to generate revenue while providing extra services to your clients, or you are interested in providing WISP (wireless internet service provider) services in your community, this paper will document the different components you will need and business issues you are likely to face.

Over the last several years WiFi (wireless fidelity) Internet hotspots have begun appearing in major metropolitan areas all over the world. Public WiFi hotspots allow users to connect to the Internet using wireless network technology in places such as airports, cafes and conference centers.

WiFi hotspots are becoming very popular with business users as they provide high speed Internet connections that can be accessed with the user's own equipment be it a laptop, PDA (personal digital assistant) or any other WiFi enabled device. Ideally, the user's WiFi device automatically detects the presence of the hotspot and configures itself to use it. The hotspot usually forces the user to login (or purchase access) through a Web page before the user can connect to the Internet. Once logged in, the user can access the Internet for any work based or recreational use they desire. The user never has to install any additional software or change the existing configuration on their device.

### **Why WiFi?**

The benefits of wireless Internet access are self evident. Some common scenarios of public hotspot usage include checking your e-mail from the outdoor terrace of your favorite restaurant, connecting to your corporate VPN (virtual private network) while waiting for your plane to board, or even getting the latest headlines on your Palm PDA while you wait in line to buy your morning coffee. These examples only begin to illustrate the freedom and productivity benefits of wireless Internet access.

The term WiFi is used to describe any of the three major wireless network standards developed by the IEEE (Institute of electrical and electronics engineers) known as 802.11a, 802.11b and 802.11g. While these standards have been in existence for a number of years, their widespread adoption began in 2001. Prior to that, WiFi technology was only seen in large enterprise networks that could both afford the required equipment and had the technical expertise to deploy it.

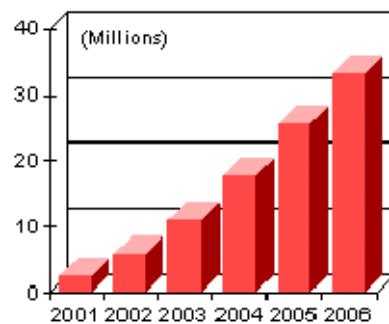
## Market Trends

The last several years have seen a huge shift in the WiFi marketplace. Equipment prices have dropped so significantly that the technology has supplanted the use of wired LAN (local area network) equipment in the home. In fact, this technology has penetrated the home market so rapidly that today every major consumer electronics retail outlet prominently features WiFi based technology in their flyers, print ads and in store displays.

The networking standards and equipment mentioned above have become so easy to use, reliable and interoperable that major retail electronics outlets such as CompUSA are selling their own re-branded (OEMed) wireless access and firewall routers for as little \$30 which can provide WiFi capabilities for an entire home or apartment. This trend is set to continue.

### Wi-Fi Home Node Shipment Forecast

Total 802.11x home nodes



Source: In-Stat/MOR 9/02

In 2002 Intel launched their new flagship Centrino chipset for mobile computing devices. In addition to offering increased power and longer battery life for devices that implement the chipset, Centrino includes built in WiFi capabilities. In 2003 over 85% of all mid and high end laptops sold included the Centrino chipset. Intel helped increase market awareness of this new technology by launching a multi-million dollar TV and print advertising campaign promoting Centrino. According to Dataquest Research, over 95% of all laptops shipped after 2005 will include WiFi capabilities.

While the hotspot provider industry is still in its infancy, according to the Gartner Group there are already 9.3 million hotspot users in the US. Analysis Research predicts that the industry will generate \$9.5 billion in worldwide revenues by 2007. As with any market containing that much revenue potential, early market leaders are emerging and creating barriers to entry for latecomers.

## Public WiFi hotspot business models

Many corporate enterprises are deploying WiFi to extend network connectivity in their facilities to areas that do not provide wired access (shop floors, boardrooms, cafeterias and outdoor areas). This technology has also opened new opportunities to existing businesses that cater to business professionals and travelers.

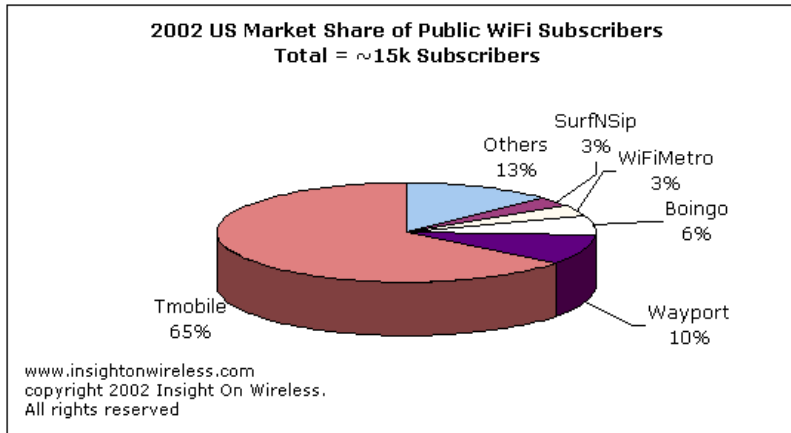
Offering Internet access via a WiFi hotspot can be used by existing businesses as either a *new revenue stream* or as a *value added* complimentary service differentiator. The type of business, operating costs and clientele of the business will determine which model is most suitable. For instance, a conference center that has an average deal size of several thousand dollars may offer hotspot access to conference organizers and attendees for no additional charge due to the relatively low overhead of a WiFi solution. On the other hand, a coffee shop with average sales of \$2 - \$5 per customer may want to increase this sales average by offering pay-for-use hotspot access in addition to increasing foot traffic, customer retention and loyalty.

Both business models consist of the same elements that must be assembled to provide public WiFi services. These are:

- **Sales & Marketing.** As with any consumer service business, sales and distribution channels are a key factor. How are you going to sell your service (and bandwidth) and to whom? Will you only sell on-line or will you have retail outlets? How will customers know where your services are being offered?
- **Distribution & Billing.** This element is tied closely to sales. Once a sale is made, how are you going to distribute user account information? How will you know when and how to stop service on empty, unpaid or delinquent accounts?
- **Field equipment.** This includes all the hardware and infrastructure required to provide service to a particular site or venue. From a business perspective almost everything in this category will be an upfront cost that you want to amortize over the life of the equipment.
- **Operations.** This includes all monthly recurring costs from bandwidth to field technicians and other support (including administrative) staff. Who will run the hotspot and what type of resources will they have at their disposal?

## Current Market Players

As of this writing, T-mobile (the wireless subsidiary of Deutsche Telekom AG NYSE:DT) is the undisputed market leader in the US. By early 2004 T-mobile had entered partnership agreements with several major retail chains to provide hotspot access to their customers. Key partnerships in T-mobile's portfolio include Starbucks Coffee Company (Nasdaq:SBUX), Borders Group Inc (NYSE:BGP) and Kinko's Inc. (recently purchased by FedEx NYSE:FDX). T-mobile currently has over 5,000 hotspots rolled out across North America.



T-mobile uses the *new revenue stream* model with its partners. T-mobile manages the hotspot installation process and operations as well as all sales aspects of the WiFi service. Users pay either a monthly subscription or purchase a block of time from the hotspot's web portal. This allows them to use their account at any T-mobile hotspot. The partner companies are not directly involved in the sales process and simply provide space for field equipment, display advertising and marketing materials.

Other carriers are also getting in on the action, choosing to partner with large well established retail sales outlets. AT&T (NYSE:T) has launched public WiFi hotspots in four states (Washington, Connecticut, New York & New Jersey) in conjunction with McDonald's Corp (NYSE:MCD) restaurants. McDonald's handles the sales and bulk of the marketing, AT&T provides the bandwidth, billing and distribution while Cometa Networks has been contracted to handle operations and field equipment deployment. In other states (such as Illinois) McDonald's uses Toshiba Corp's (PK:TOSBF) Surf Here service to provide field equipment and operations components.

Hotel chains such as Marriott Intl Inc. (NYSE:MAR) and Starwood Hotels & Resorts (NYSE:HOT) use WiFi hotspots in the *value added* model, offering free WiFi access to guests staying at select properties. Over 1,700 hotels in the Marriott chain will be wireless at the end of their initial roll-out, while the Starwood group plans to bring 750 properties online by the end of 2004. These companies either handle everything in-house or contract aspects of deployment and operations to companies such as Cometa Networks, Wayport, Stay Online or STSN.

Verizon Communications (NYSE:VZ) is also using the *value added* business model. As the largest hotspot provider in New York City, Verizon WiFi access is free to all Verizon Online ISP customers.

Several regional hotspot providers have gone from hobbyist endeavors to commercial solutions. Regional hotspot providers are branching out into national networks that partner with venues in specifically targeted areas. Some of these networks include the Surf and Sip Network based in the San Francisco area and HotSpotzz in California and Utah.

Larger national and international WiFi network providers make up the rest of the market players. These include companies like Boingo Networks, Toshiba's Surf Here, PacificWiFi and Airpath. These companies provide various aspects of distribution, billing and field equipment to venues in exchange for monthly fees and/or revenue sharing. Venues become clients of these companies and their VARs (value added resellers) in order to provide a WiFi hotspot at their location that allows roaming and online billing with very little configuration. Roaming agreements allow end users of one network to use hotspots operated by other network providers through backend pre-established chargeback agreements between the network providers.

At the other end of the spectrum, local citizens have banded together to provide free network access in their communities such as the famous SeattleWireless project. CWNs (Community Wireless Networks) have sprung up everywhere from Seattle Washington to Sydney Australia. The CWN community is responsible for the best WiFi consumer product testing anywhere in the world and many of the features provided in today's commercial hotspot hardware and software is based on work by early CWN pioneers. Unfortunately, CWN coverage in most areas remains spotty. CWNs do not concentrate on providing free WiFi Internet access; they are trying to provide a free wireless network infrastructure that bypasses normal telcos and cable companies.

Company	Estimated subscribers	Number of locations	Financing
Boingo	1,000	700 (Most are Wayports and SurfNSip locations; about 60 free locations)	Well Funded. Raised \$15M in Dec 2001. Funding should last until 2004
Joltage	100	50 (Most are in NYC)	Self-Funded. Is looking for Series A investment
SurfNSip	500	120 (Most are in CA)	Self/Angel Funded
Tmobile	10,000	1300 (Starbucks in 15 metro areas; and 27 Airports)	Deep Pocket Telecom Incumbent
Wayport	1,500	500 (Hotels and 9 Airports)	Raised over \$105M in multiple rounds
WiFiMetro	500	75 (Most are Bay Area, CA cafes)	Company shut down in late July
Source: Companies' websites, Press announcements, Executive interviews			

**2002 WiFi network provider breakdown**

## Putting it all together

The four components of a hotspot solution sales & marketing, distribution & billing, field equipment and operations must be properly assembled whether your company is a large carrier or a single location. Aligning these elements can be challenging and there is no "one size fits all" solution. As with any business, costs must be compared carefully to prospective revenue.

The major fixed costs in a hotspot deployment are field equipment and bandwidth. Profit sharing arrangements, payment processing fees, marketing, support and administration are the major variable costs that must be considered. Each of these elements will be explored below.

A hotspot's infrastructure should allow end users to easily connect to the system using standard WiFi equipment. Your WiFi signal must reach everywhere you wish to provide service, and at sufficient signal strength. Venues need to be equipped with marketing material and may also offer direct sales of time and bandwidth through cards or coupons. The wireless infrastructure should provide AAA (authentication, authorization and accounting) functions, sufficient Internet bandwidth and security required for proper operation. Roaming agreements with other network providers should be considered. Onsite, online or telephone end user support may also be required.

Each hotspot generally has its own captive portal to which end users are restricted until they pay and/or authenticate. Many portals also provide "walled garden" features which let guest users browse certain web sites for no charge. Custom branding, advertising and e-commerce functionality are other common features found in many hotspot portals.

## **Sales and Marketing**

The most successful hotspots are ones that build on both a good location and a good brand. Don't underestimate the power of brand. WiFi hotspots are in their infancy as a revenue source and brand may be a determining factor in the inevitable consolidation that will occur in the industry. Plan to build and maintain your brand throughout all aspects of the hotspot business from portal design to support calls.

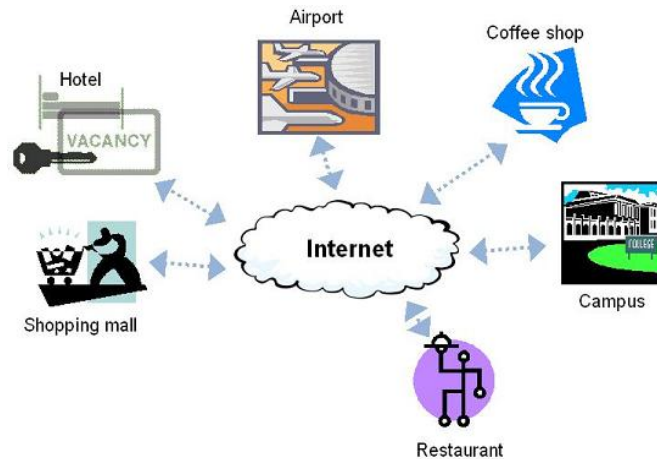
### ***Venues***

Location, location, location. Good venues are the key to a successful hotspot business. However, you must understand the market before evaluating the potential of a particular location. As of early 2004, there are three major categories of WiFi hotspot users. The most successful hotspots are located in venues that cater to these specific users.

Business professionals, college students and early adopters (a.k.a. *power users*) are the three groups that are most likely to already have WiFi enabled equipment. They are typically mid to upper income individuals, spend the majority of their time in major metropolitan areas and have disposable income (or expense accounts) to spend on the service. These markets are large and as further penetration of WiFi devices continues in the general population, the market for WiFi hotspots will grow.

Venue usage patterns, atmosphere and physical layout are also important factors when considering a prospective venue. An ideal venue will cater to the markets above and patrons will spend 15 minutes or more on average in the vicinity of the venue. End users must have a chance both to encounter the marketing for the hotspot as well as have the

time and requisite frame of mind to use it. They must also have the required equipment with them.



### Typical Hotspot Venues

Airports and hotels are the traditional golden opportunity hotspots. Their patrons are generally middle-upper income and they tend to already own the necessary equipment. Airports and hotels have the added benefit of catering to business travelers, which is currently the market group with the highest WiFi equipment penetration. Cafes and restaurants are often seen as prime locations, although you really need to understand the usage pattern of each particular venue when evaluating these types of establishments. Less obvious locations that have proven very successful are waiting rooms for doctors, dentists and mechanics, especially those located in financial or business areas. Anywhere business people have to sit and wait is generally a good location.

When initially evaluating a venue, you want to ask the following questions:

- Which relevant market(s) does this venue cater to?
- Are my target users likely to have WiFi enabled equipment with them when they visit the venue?
- Would more patrons bring WiFi enabled equipment to the location if they knew it offered Internet access?
- Do patrons of the venue spend more than 15 minutes on average in the vicinity of the venue?
- How many patrons visit the venue per day/month/year?

Costs associated with setting up a venue must also be considered. In some locations one WiFi antenna will provide sufficient coverage for the entire venue, others may require many more. Try to determine if the revenue from the venue will be in line with cost of equipping it. You must also make sure your pricing model fits the venue. Selling monthly subscriptions at a truck-stop hotspot won't get you very far.

Once your brand strategy is decided, you must create marketing materials for distribution within the venue, ranging from signs informing potential customers about the service (and roaming partners) to informational material on how to buy the service and use it.

Depending on your infrastructure design, each venue may have its own captive portal that end users will use to login to the hotspot. Think about how your brand goals will fit in with this and how you might increase revenue by offering promotions or advertising through the portal.

## Distribution & Billing

Distribution and billing systems may remain relatively unseen by the end user, but they are often the biggest differentiator between various hotspot operators and network providers. To understand distribution in the context of the hotspot business, consider that what you are selling is not WiFi access or bandwidth, but rather a username and password which is valid for a certain amount of time (or for a certain amount of use) at one or more locations. Next you must decide how you will sell it, deliver it, bill for it and manage the entire process.

Distribution tends to occur either online or as a cash sale at the venue itself. It is generally easier to handle billing and distribution of user credentials online, but this doesn't allow the same type of venue participation and revenue sharing opportunities available when combining online sales with the onsite distribution of coupons or the sale of prepaid cards. One of the major variable costs to consider when using an online distribution and billing system are the transaction charges you may incur for processing online payments.



**Access can be sold either online or as a cash sale of prepaid time**

Technical management of all these elements falls under the auspices of AAA (authentication, authorization and accounting) systems. Choice of a AAA system should be based on your business objectives. The AAA system may place limits on how you can sell your service; some of the questions you may want to ask are:

- Does it support both prepaid accounts and subscriptions?
- Can it integrate with online billing systems?
- Can users see their usage information online?
- AAA systems may limit who you can partner with, i.e., does the AAA system support roaming features with major network providers?

AAA systems can also limit the features you can offer your end users; You will want to know if a particular system will allow you to create a walled garden (offer browsing of certain websites for free) or offer other features.

Offering roaming agreements with other WiFi hotspot providers or networks increases the value of the service you are selling by allowing your end users to access WiFi hotspot services in other locations thus freeing them from having to purchase multiple accounts with different providers. Roaming agreements can also bring new customers to your venue looking for compatible access and hotspots generally bill roaming users at premium rates.

An important aspect of distribution and billing is reporting. When evaluating management systems make sure you will be able to generate the reports you will need to measure the success of your business and to fulfill any partnership or roaming agreements you have committed to.

## **Field Equipment**

Selecting and properly deploying the correct field equipment will let a hotspot provider deliver the quality of service its end users expect at a reasonable price. Network design skills are essential as is knowledge of WiFi equipment and specifications. RF (radio frequency) transmission and reception is not something many current network designers know well.

Providing hotspot services in a single location can be as easy as plugging in a small box and printer to your existing high speed Internet connection, or as complicated as you wish to make it. Adding different physical locations to a single venue or coordinating multi-venue setups can be much more involved.

The network elements that make up a WiFi hotspot are:

- **Internet bandwidth.** How will you get Internet access to your end users? Will multiple venues use the same Internet gateway or will they each have their own?
- **AAA system.** Authentication, authorization and accounting functionality controls who, when, where and for how long an end user can use the service. AAA can be located at various points in the network infrastructure.
- **Access points (APs) and antennas.** Getting WiFi signals to your end users is done using APs and antennas. Indoor and urban environments can present significant challenges for those uninitiated in RF transmission.

### ***Internet Bandwidth***

The largest field equipment cost is generally providing the venue with Internet bandwidth. If you have more than one venue you should decide whether you will have centralized Internet access and connect each venue via physical LAN, VPN or long range WiFi links. Alternatively, you can use ADSL, cable modem or dedicated circuits such as T1s at each venue. Examine the costs of implementing different options. Sometimes it

can be much cheaper to consolidate hardware and Internet bandwidth at hubs and use WiFi to distribute the functionality where it is needed, though this may require more significant upfront costs.

Bandwidth partnerships can be essential. Simply signing up for any local high speed ISP (Internet service provider) might not be enough. Many standard ISP end user license agreements do not allow the resale of bandwidth. All the national carrier class ISPs (MCI, Sprint, AT&T, etc...) offer reseller programs which may entitle you to rebates or additional revenue. Don't forget to research local ISPs as many offer competitive resell programs.

Not all ISPs are created equal. Many corporate IT managers have learned this the hard way. Price isn't the only factor that affects the bottom line. Repeated or prolonged Internet outages at your venues can have a devastating effect on your hotspot business. When comparing ISPs, find out how long they've been in business, what their system availability has been over the past several years and what type of SLA (service level agreement) they are willing to provide you.

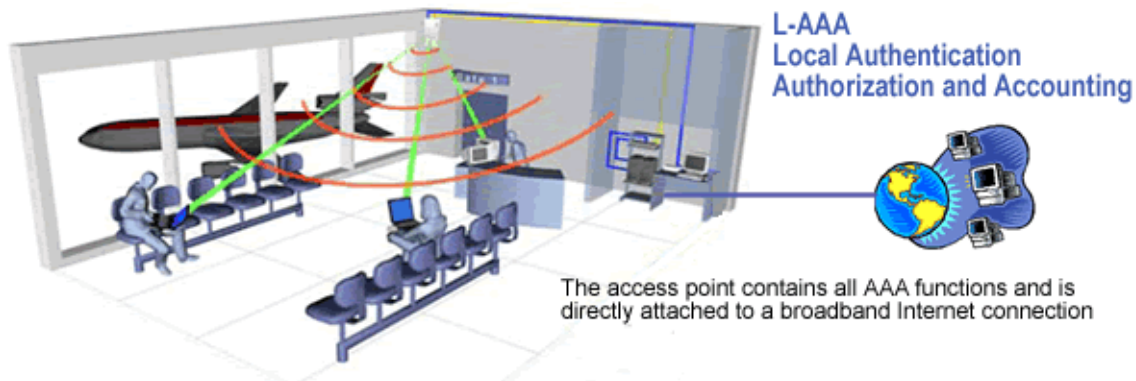
Service level agreements are guarantees from an ISP that unscheduled downtime of their service will not exceed an agreed limit, usually measured in minutes per month. SLAs have become very watered down over the years and many ISPs offer no SLA for ADSL or cable modem services. However, if you are spending a substantial amount of money with an ISP, use this as leverage to negotiate a better SLA. If you are worried about the service level of an ISP and they are unwilling to bet on their own performance through an SLA, you may want to continue shopping around.

### ***Authentication, Authorization & Accounting (AAA) Systems***

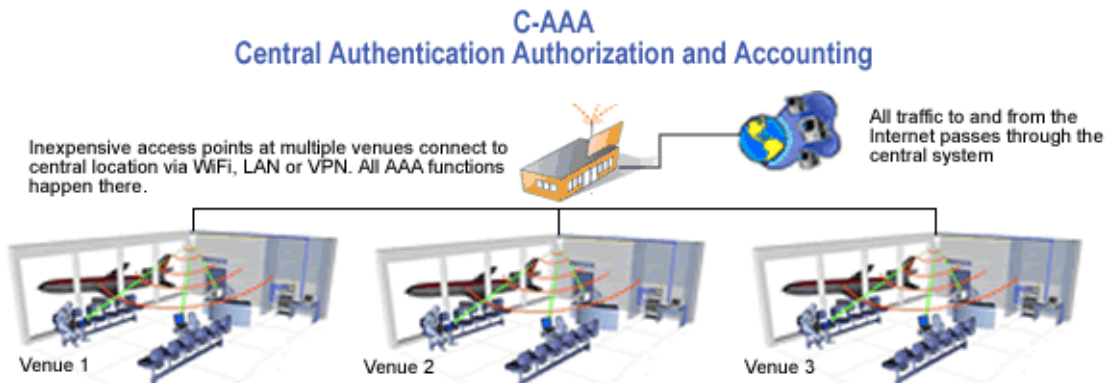
AAA systems are the glue that ties together all the other components of a hotspot solution. They authenticate end users to make sure they have a valid username and password; they allow each user to use only the resources to which they have been granted access and they keep track of how long a user accesses each resource and from where.

There are three main models for deploying AAA systems in hotspot network design. As you might expect, each has its benefits and drawbacks.

- **Local AAA (L-AAA).** This is where all AAA functionality takes place within individual access points like the Proxim Orinoco AP-2500 or in a device that consolidates AAA functions for multiple APs in a single venue such as the Dlink DSA-3100. Many hotspot-in-a-box devices employ this model (although most can also be used as an access controller in a D-AAA model network). These devices provide very simple installation, setup and maintenance but may limit how you can sell your services as well as the possibility of roaming between venues or with partners.

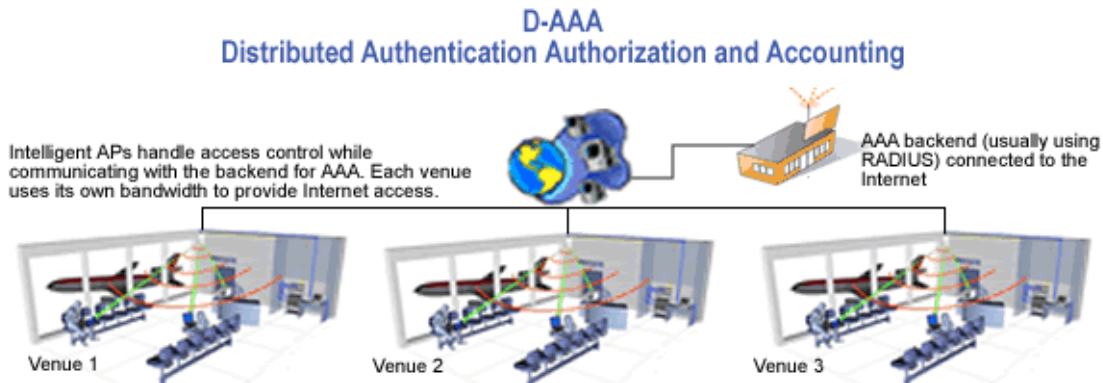


- Centralized AAA (C-AAA).** Centralized authentication, authorization and accounting systems consolidate all AAA functions for multiple venues in a central location. This model is most appropriate for WISPs (wireless internet service providers) and hotspots that have a large number of different physical areas that need coverage, but have centralized Internet access, such as neighborhood/community access, hotels, airports or any campus. All outbound and inbound traffic for end users in each venue needs to pass through the central location before being routed to its final destination. The advantage of this model is that you can use very cheap and dumb access points while consolidating security functions in a central location. To fully appreciate the significance of this, try running an IDS (intrusion detection system) at multiple venues on a network using one of the other models.



- Distributed AAA (D-AAA).** Distributed authentication, authorization and accounting systems are a hybrid of L-AAA and C-AAA; as such D-AAA tends to offer more flexibility (and complexity) than any of the other models. In these systems, authentication and authorization are handled jointly by an access control device at the venue and a central AAA server on another network, with most of the accounting functions performed by the central server. D-AAA systems require high speed Internet access at each venue and a central AAA server that is accessible all the venues (usually via the Internet). This model allows venues to take advantage of cheap broadband Internet access while still centralizing core features to easily manage multiple venues. D-AAA systems also require a fairly

intelligent access controller at each venue that is capable of communicating with the central AAA server (usually via the RADIUS protocol).



With the emergence of hardware that supports the D-AAA model, a number of managed AAA services have emerged allowing backend network providers such as Boingo, Airpath and Toshiba's Surf Here to sell hotspot-in-a-box devices capable of being easily installed and providing instant integration with their respective backend managed AAA services.

AAA systems are also responsible for other security feature implementations such as firewalling and VPN connectivity. When evaluating hardware or software, be sure you understand which security features it implements and how it implements them. Some questions you should ask include:

- Can it restrict certain inbound and outbound traffic?
- Can it redirect the appropriate network traffic?
- What firewall features are implemented?
- Can it prevent end users from talking to each other?
- Can it handle advanced authentication protocols such as 802.1x?

### ***Access Points & Antennas***

Access points are devices that convert RF (radio frequency) signals to and from end users into standard network communications. Most APs come with attached antennas, but many of these can be replaced or supplemented with external antennas that can increase the range of your hotspot service.

Your AAA system will determine how smart (and expensive) your APs need to be. The physical layout of your venue, the broadcast power of the APs and the characteristics of your antennas will determine how many APs and antennas you will need to cover a given area.



### WiFi enabled products

WiFi signals come in 3 flavors, but most access points can only use one or two. These three flavors are standards set out by the IEEE for wireless networking and they are:

- **802.11a.** This WiFi standard operates in the 5GHz frequency range and uses a technique called OFDM (orthogonal frequency division multiplexing) for transmission/reception. This standard offers up to 54Mbps data transmission speeds. The 802.11a standard has not yet become very popular and is not offered at many hotspots. Those that do generally also offer one of the other standards listed below.
- **802.11b.** This is the most widely deployed WiFi standard to date. Most references to WiFi equipment refers 802.11b unless otherwise stated. This standard operates in the 2.4GHz range and uses a technique known as DSS (digital spread spectrum) for transmission and reception. This standard only offers 11Mbps total data bandwidth, but this is more than enough for hotspot Internet access.
- **802.11g.** This is the newest standard of the bunch and like 802.11a, provides 54Mbps transmission speeds using OFDM, but operates in the 2.4GHz frequency range. A nice feature of this standard is that it is fully backwards compatible with 802.11b so all 802.11g devices can talk to 802.11b access points.

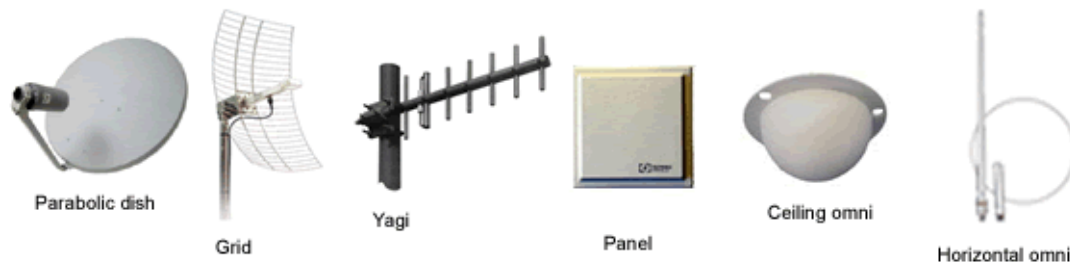
Most hotspots use 802.11b equipment as it is cheap, widely deployed and fully compatible with 802.11g devices. As end users should not be allowed to consume anywhere close to 11Mbps of bandwidth, the limitations of 802.11b are not an issue. On the other hand, conference centers, trade shows and other similar hotspot venues may want to allow end users to communicate between themselves (for things such as file transfers) or access certain local services (such as streaming video of speakers) at higher data rates and may thus choose to deploy 802.11a or 802.11g equipment. Some access points offer both 802.11a and 802.11b access, but most smart APs used in L-AAA and D-AAA systems offer only 802.11b features.

The 2.4GHz frequencies used by WiFi equipment are unlicensed in North America, meaning you can setup a WiFi network without seeking approval or licenses from the government. The major drawback to this is that you are not guaranteed any quality of service and interference from other devices can not be controlled. In fact, aside from

other WiFi equipment that may be deployed near your hotspot, you can expect interference from things such as microwave ovens, cordless phones and Bluetooth devices, all of which transmit in the 2.4GHz band.

The US FCC (Federal Communications Commission) defines power limitations for wireless LANs in FCC Part 15.247. The FCC caps the power of a transmitter and antenna solution (equivalent isotropically radiated power) to 1 watt of power. It may not sound like very much, but most hardware falls well within this limit. European standards vary from country to country, but in general are more restrictive. In fact, some countries do require licenses for any public or commercial use of WiFi networks.

### Different WiFi antenna types



Antennas come in two basic designs, either omni or directional. Omni antennas broadcast (and receive) their signals from 360 degrees (generally either along a vertical or horizontal axis, although there are omnis that do both). This means that all directions from the center of the omni are transmitted to equally. Directional antennas concentrate their power in a much narrower beam allowing them much better gain in whichever direction they are pointed. Directional antennas are mostly used for longer range transmissions between APs; two directional antennas pointed at each other will be much less susceptible to interference when compared with omni antennas.

Antenna placement can be crucial in getting a WiFi signal from your access point to end users. Most APs come with one or two low gain omni antennas; on lower end models these are not replaceable, though most mid and high end access points allow you to attach at least one external antenna. Most APs with multiple antenna hookups can be used in diversity mode which lets the access point use whichever antenna has the best signal to the target, thus increasing range, bandwidth and link stability. One can further increase the range of hotspot coverage by using multiple APs in “repeater” mode which lets a second AP act as a range extender for the master AP. Not all APs support this feature and those that do generally can only be used in this manner with equipment from the same manufacturer.

Any equipment placed outdoors should be properly protected whether it is an access point or antenna. Outdoor APs should be deployed in NEMA (National Electrical Manufacturers Association) approved enclosures. Heaters and fans can be installed if required in your region. Outdoor antennas should be wind rated appropriately for their install location and lightning protection should be installed on most antennas mounted

outdoors. POE (power over Ethernet) injectors can be used to combine LAN and power runs to an outdoor access point into a single wire.

## Operations

Running and maintaining a hotspot infrastructure can be challenging and many first time hotspot operators and venue owners underestimate the costs involved in ongoing operations. These costs can add up quickly and if not addressed, customer satisfaction, loyalty and retention will decrease, as will revenue.

Operational functions fall into four categories:

- **Installation.** This involves conducting a site survey of the venue to measure interference from other devices in the area as well as determine how many access points and antennas will be required and where they should be positioned. Once this is complete, the equipment should be ordered, installed and a post-install site survey should be conducted to ensure your signal is reaching everywhere you want to provide access.
- **Maintenance.** WiFi equipment is mature and shouldn't require any more onsite maintenance than other networking equipment. An automated network monitoring system is vital, as is staff to investigate and resolve any reported technical issues. WiFi signals are very sensitive to interference which may increase over time; they can also be affected by growing foliage or architectural changes that may occur in the area. WiFi links and access point coverage should be re-evaluated every 6 to 12 months.
- **Support.** Due to the nature of hotspot services, end user technical support should be instantly accessible if available. End users vary greatly in technical ability and hardware/software configurations. Several AAA service providers such as Toshiba Surf Here and AirPath offer end user technical support through call-centers. Online access to live help, billing information and detailed help files can reduce end user support costs.
- **Administration.** This is a catch all for other activities and costs required to run one or several hotspots. This includes HR costs, phone service and any other items you require to provide service at a particular venue or to run a backend network.

## Conclusions

The enormous investments in WiFi hotspots currently underway by the large carriers in New York, San Francisco and Seattle coupled with the incredible market penetration of WiFi technology into homes and businesses is indicative of the large user base that can be targeted to for these services.

This leaves two questions; will end users be willing to pay for access to hotspot services? And, what's likely to happen to the hotspot marketplace? We can infer an answer to the first question, but the second can only be guessed at.

From phone service and airline tickets to magazine subscriptions, businesses have long been accustomed to paying premiums for services that enhance productivity or increase business potential and are thus likely to pay for employee hotspot access. The remainder of the market is not as easy to categorize. There is a question as to whether other end users will be willing to pay for an ISP account at home and then another for WiFi access in public locations. Companies like Verizon are taking advantage of this by providing free WiFi access to all their monthly ISP subscribers in metro areas like Manhattan. Other market leaders such as T-mobile are betting that the same market that pays a huge premium for flavored coffees will pay a small per use or monthly charge for WiFi Internet access while they drink their java.

In the near term it appears as though the WiFi marketplace will remain fairly fragmented. There will be the large market players mentioned above, the independent network providers that sign up and aggregate services for a network of venues and lastly, independent venues providing service on their own behalf. What will ultimately happen to the market is anyone's guess, but there are some the factors to consider.

Cell phone providers have been promising high speed Internet access via their headsets for years. This functionality has yet to emerge and the existing (slow) data services offered are extremely costly both for the end user and the network provider. Anyone who has used their cell phone as a modem with their laptop can attest to the poor performance and unreasonable cost of these services.

The hotspot marketplace appears to be analogous to the emergence and evolution of other ISP services. When dial-up ISPs initially emerged for the home user market, there were three types of players in the ISP market space; the large national ISPs such as CompuServe, IBM and AOL, the smaller regional ISPs including those run by the baby Bells and finally, mom and pop ISPs that used local expertise and service to penetrate markets that the others couldn't reach. As the dial-up ISP market heated up, many of the smaller ISPs were acquired by larger competitors for their customer bases.

The development of broadband Internet services in the residential market may be useful in examining the effect of early adoption and regional availability of these service types. The emergence of cable modem and ADSL services for residential users changed the way many ISPs did business. Whereas dial-up services were available to anyone with a phone line and modem (owned by the end user), broadband services cost much more to use and deliver while requiring the end user to rent equipment from the ISP and thus leave the ISP with the responsibility of installation, operation and maintenance of end user equipment.

Also, unlike dial-up services broadband is not available to everyone. The end user must be located within a certain distance from key infrastructure equipment to be serviced, depriving large residential areas of coverage. Despite all of these drawbacks, ISPs and end users have embraced broadband services in large numbers. Many new ISPs only offer broadband service, forgoing the cost of dial-up equipment while going after more lucrative and popular broadband accounts. In fact the emerging class of ISPs known as

WISPs (wireless Internet service providers) provides residential broadband services delivered to the end user via WiFi signal. These are particularly strong businesses in areas where broadband access is not available.

WiFi hotspot services are likely to follow a similar path as both dial-up and broadband ISP services. Every day the market base for hotspots grows as WiFi equipment continues to become ubiquitous in both business and home environments. Owning the rights to provide service at prime venues will probably determine the ultimate success of network providers.