Operations support system (OSS) requirements and solutions for carrier-grade Wireless LAN services

One of the major challenges in offering a carrier-grade Wi-Fi service is to choose and deploy an effective OSS infrastructure. This paper discusses the requirements for customers, service providers, network operators, and venue owners, and provides recommendations for service providers and network operators evaluating different OSS options.

Monica Paolini · Senza Fili Consulting · November 2003

Senza Fili Consulting LLC
www.senza-fili.com
info@senza-fili.com
(425) 868 4100

The Operation Support Systems (OSS) challenges for WLAN services

Wireless LAN (WLAN) access is finally coming of age. The number of hotspots is growing rapidly around the world (with over 10,000 in the US alone), as users are increasingly eager to use the service not only in airports, coffee shops and hotels, but also on trains and in underground stations, in RV parks, and marinas. As WLAN access expands to new types of hotspots or to wider hot zones, and as multiple networks and service providers share the wireless infrastructure, more complex WLAN topologies have started to appear.

The WLAN infrastructure is growing in complexity

Airports are a good example of this ongoing transformation. Initially, WLAN access was limited to an airline lounge or a couple of gates, and a single service provider offered the service through a monthly subscription or a credit card payment. The network was typically used only for public access and the over-the-air link was left unprotected. This relatively simple WLAN infrastructure is becoming more complex, as the number of services increases and as the requirements from users, service providers and venue owners have become more sophisticated:

- **Coverage.** Areas covered by the WLAN have expanded, often to include entire terminals or airports.
- **Roaming.** The increasing number of roaming agreements results in several service providers offering public access through the same network operator.
- **Security.** Robust security solutions, such as WPA, are now available to protect all users, but they require direct involvement of service providers and network operators to enable mutual authentication and encryption keys management.
- **Consistent service.** Service providers want to label the service, charge the user through a single bill, and offer the same level of service and client interface that is available within their own network.

- **Location-based services.** The airport may request to provide location-based information and services (e.g. information about flight departures, airport services) to the travelers.
- **Client interface.** Users increasingly demand a robust, easy-to-use interface and a secure connection, while retaining the ability to select their favorite service provider or use alternative security solutions, such as their company's Virtual Private Network (VPN).
- **Multiple virtual networks.** Besides public access, WLANs may provide services to airport concessions, airlines and security agencies, thus creating the need for multiple virtual networks, all supported by the same WLAN infrastructure.

The effects of the increased complexity at the hotspot level are magnified by the growth of the domestic footprint and its international expansion. The establishment of roaming agreements among service providers based in different countries has suddenly given international access to subscribers. It has also increased the back-end burden for service providers and network operators alike.

Compelling, carrier-grade services are critical

Several mobile carriers, fixed operators, Wireless ISPs (WISPs), and, in some cases, venue owners, are offering or planning to offer Wi-Fi access, and are becoming increasingly aware of the challenges that WLAN services pose. Once they have established a footprint, by building their own infrastructure (e.g. T-Mobile, BT Openzone, Wayport) and/or by entering roaming agreements (e.g. Sprint, AT&T Wireless), service providers need to ensure that they are offering a compelling, carrier-grade service to their customers. This is a crucial capability for service providers to attract subscribers, differentiate themselves from competitors who may offer free access, and avoid commoditization of the service.

A robust OSS is a prerequisite for a carrier-grade WLAN service

The task of managing the WLAN infrastructure and services to the subscriber has proved to be more complex than initially expected. As a result some subscribers find it too difficult or time consuming to get connected at hotspots, and service providers have only limited back-end functionality. Adoption of an effective WLAN OSS is a crucial step to ensure that WLAN can become a carrier-grade service, that has the same reliability and level of customer support as the other services offered by the service provider.

WLAN OSS is challenging and increasingly complex

The challenges that a WLAN OSS faces are several. WLAN access is a service that is not yet mature and that is rapidly evolving. Relying on a relatively new technology that is used in multiple environments (e.g. at home and at work, in addition to public hotspots), users often need additional support to learn how to use the service in a new environment and avoid software conflicts. The potential for Value-Added Services (VAS) creates additional requirements for future compatibility that are often difficult to assess. The lack of widely accepted standards for Authentication, Authorization, and Accounting (AAA) and security and the need to integrate with the OSS for existing services (e.g. voice services) adds complexity to the adopted OSS solution. To complicate matters further, the presence in the market of different players (e.g. venue owners, fixed operators, mobile operators, WISPs) translates into different integration needs, as the WLAN OSS typically coexists with different legacy systems. The emerging complex roaming infrastructure increases the number of players that need to exchange user data information and to process payments. At the wholesale level there is still considerable uncertainty as to the metric (volume, time-metered, or daily access) to be used, requiring network operators to collect different sets of data for different service providers. Finally, the need to establish interworking with cellular networks, will create additional requirements and a closer cooperation between service providers and network operators.

This white paper examines the OSS requirements that service providers, network operators, aggregators and clearinghouses have to meet to address these challenges, and provides recommendations on how to evaluate and select an OSS. The requirements are assessed from the viewpoint of the value chain actors: subscribers, corporate clients, venue owners, network operators, and service providers and. Recommendations are based on the outlined requirements and on the demand that we expect to arise from future services.

OSS for WLAN: a definition

To clarify the scope of the white paper, it is useful to define the five functional areas that WLAN OSS encompasses (Figure 1). They include billing and customer management that are sometimes defined as Business Supporting Services (BSS).

WLAN access is often an add-on service and it uses roaming extensively. These two features dictate specific requirements for WLAN OSSs. As WLAN is often offered as part of a package that includes other services (e.g. in addition to cellular voice and data services), a WLAN OSS needs to be integrated to some extent with the service provider's existing OSS. Furthermore, the service provider may desire that some of the OSS functions, such as customer service and billing, be largely performed by the existing OSS. Other functions, such as roaming services, network management, Quality of Service (QoS) implementation and security, are specific to WLAN services and have to be addressed separately.

As WLAN access through roaming partners is likely to become prevalent, service providers do not always operate their own WLAN hotspots and some of the OSS functions (e.g. network management) are performed in large part by the network operator (which may or may not be a service provider) (Figure 2). Two types of intermediaries may interface service providers and network operators and be responsible for some OSS functions:

Billing	Customer Management	Network Management	Service Provisioning	Service Assurance
Event management Rating, discounting Roaming retail billing Roaming wholesale billing CDR exchange with roaming partners Invoicing Taxation Collection Fraud management Micropayments	CRM Customer service Customer self service Call center management Trouble reports	Network planning Resource management Configuration management Remote management Security and authentication management	Order management Workflow management Service activation Network provisioning Network inventory Policy management	Performance management Fault management Trouble ticketing SLA management QoS implementation Testing Reporting and data analysis

Figure 1. OSS functions

- Aggregators that bring together network operators and service providers through roaming arrangements geared to increase traffic and optimize the use of the wireless infrastructure.
- Clearinghouses that facilitate the transmission of usage and billing information and offer financial settlement services.

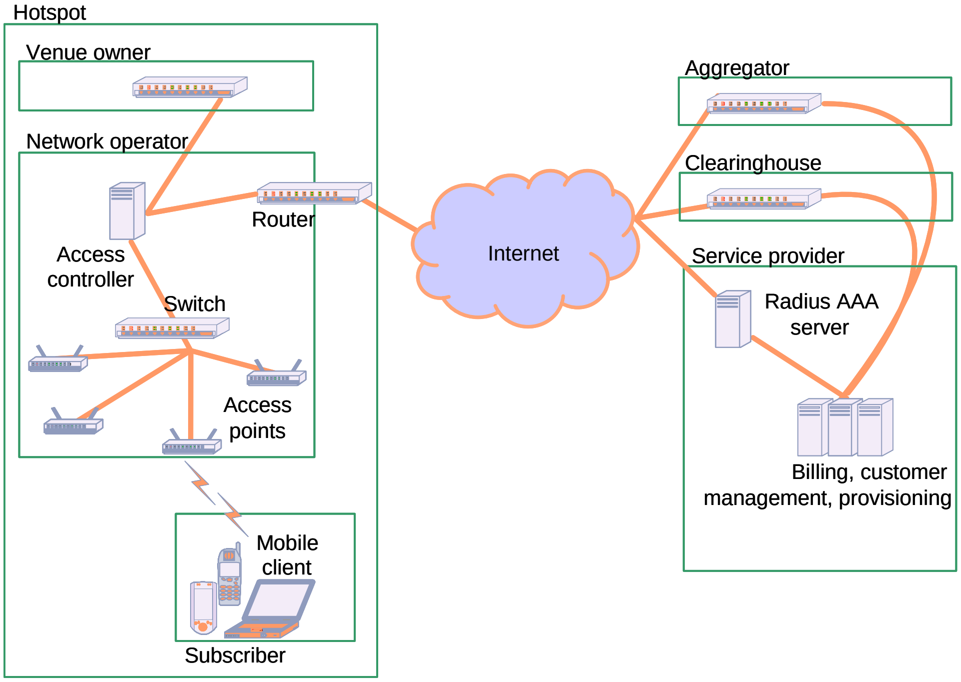

Figure 2. Players and relationships involved in a hotspot session

Requirements for a carrier-grade Wi-Fi service

The following sections discuss the requirements for end-users, corporate clients, venue owners, network operators and service providers.

End-user requirements: ease of use and consistent service

Using WLAN in a public hotspot can still be a frustrating or time consuming experience. To start, it is often difficult to locate the coverage area and, once identified, the user needs to select the appropriate network manually if multiple networks are available. The authentication process is often inconsistent, slow, and, if the user does not have a subscription with the service provider, requires entering credit card and billing address information. The limited availability of roaming services creates the need for the frequent user to maintain different accounts with different service providers to have access to a wide set of hotspots. While current Wi-Fi users are enthusiastic about the service, greater ease of use and consistency are necessary to attract less tech-savvy, but more numerous, users.

The key subscribers' requirements to achieve these goals are the following:

- **Quick negotiation of connections.** The user needs to be able to select the preferred Service Set Identified (SSID) and service provider, and get authenticated very quickly (less than a minute).
- **Easy to use interface for AAA.** Regardless of the local network operator, the subscriber needs to find a familiar, consistent, easy-to-use interface provided by the service provider.
- **Robust security.** The over-the-air link has to be secured while allowing the subscriber to use alternative security solutions, such as VPN (Figure 3). It is worth noting that robust security solutions such as Wi-Fi Protected Access (WPA) and, in the future, Microsoft Wireless Provisioning Services (WPS) require support from the network operator and service provider and thus, unlike VPN, cannot be adopted unilaterally by the subscriber.
- **Single bill.** When roaming on a partner's networks, all the fees incurred have to be charged to subscriber's main account.
- **Information about hotspot locations and prices.** When multiple options are available (e.g. multiple network operators, or service available through roaming agreements from different service providers), the user needs to have access to information about pricing, service features, and coverage area and be able to select the preferred connection option.
- **Pricing flexibility.** Different pricing options are necessary to attract users with different requirements. Heavy travelers may choose a flat fee price, while the occasional user may prefer a per-session or per-minute charge, or a pre-paid account. Subscribers with high usage requirements may also opt for premium services enabled by QoS which will give them a higher priority in using the bandwidth available.
- **Management of own account online.** Subscribers find it valuable to access information about their account and their usage of the service online.
- **Effective customer support.** Customer support needs to be available initially to educate the user, and later to address more complex problems.

WPA/802.1x	WPA is a Wi-Fi Alliance de-facto standard that overcomes the security vulnerabilities of WEP. It provides support for mutual authentication through 802.1x, dynamic encryption keys through TKIP, and for AAA functionality through RADIUS.
802.11i	IEEE 802.11i is a proposed standard that will be backward compatible with WPA and will provide support for a more powerful encryption scheme (Advanced Encryption Standard, AES). Ratification of the standard is expected by the end of 2004.
VPN	VPN is a tunneling protocol that protects data in transit over a wireless or wired link through encryption. It is currently widely used to secure WLAN connections, after the initial authentication.
EAP	Authentication protocol that provides mutual authentication (the network is authenticated by the user, and the user by the network) using several credential types, such as passwords, SIM, and digital certificates.
PEAP	Extensible authentication protocol that can be used in conjunction with EAP to provide further protection.
WPS	Microsoft provisioning platform that includes WPA, 802.1x and PEAP, that provides increased security and an improved interface. WPS is expected to be available in 2004.

Figure 3. Wi-Fi security: standards and solutions

Corporate client requirements: security, wide availability and monitoring capabilities

Business users are, at least initially, the most attractive market segment. They travel frequently, often with a WLAN-enabled laptop, they have extensive data connectivity needs, and the cost of their WLAN subscription can be easily justified by productivity gains.

Frequently, it is their company that directly negotiates the account for all employees with the service provider and wants to ensure that wireless access while traveling is compatible with corporate guidelines. In addition to the requirements of individual subscribers discussed in the previous section, business users often require additional services, dictated by the IT policies of their company:

- **Security.** While corporations may in the longer term want to make specific corporate services available to their employees while working remotely, at present their major preoccupations are to ensure secure connections and adherence to company policies (e.g. with regards to Internet access). The ability of a service provider to offer secure authentication and access, and to allow the use of corporate VPN tunneling is necessary to gain acceptance, as a security breach may compromise not only the employee using WLAN services, but it could jeopardize the entire company.
- **Wide footprint.** Corporate customers will need to have access to a wide network of hotspots, including most airports, convention centers, and hotels. At all locations, a consistent service is expected. As not all service

providers will be able to have their own infrastructure in those locations, it is necessary they develop roaming partnerships with the network operators that manage these hotspots to offer an attractive service.

- **Customer support.** Effective customer support has to be available to address the corporate users needs. This is key to reduce the impact that the service will have on corporate internal IT support and to ensure customer satisfaction.
- **Advanced account management ability.** Corporate accounts will require detailed usage and billing information both at the individual user and at the company level for internal monitoring purposes.

Venue owner requirements: reach the subscriber and minimize infrastructure maintenance

Venue owners welcome WLAN hotspots on their property for three primary reasons:

- Revenue opportunity
- A service to their customers
- A means to reach visitors or customers and offer information and services.

Venue owners are increasingly less involved in the direct management of hotspots, relying instead on network operators to deploy and manage the WLAN. As a result, they want to minimize the intrusion of the wireless infrastructure on their operations. To meet their expectations, WLAN services need to meet these requirements:

- **Hassle-free infrastructure.** High reliability and remote network management are necessary to ensure that the service runs smoothly in the background, without too many inquires from subscribers, or visits from the network operator.
- **Location-based services and branding.** The venue owner may want to brand the service, along with the service provider, in the splash page, or offer relevant information and specific services (e.g. check out in a hotel, flight information at an airport) to its customers. If micro-payments are required for those services, the OSS must support a framework for charging the subscriber through the service provider bill. As some location-based services may be free to all customers and may not require authentication, virtual separate networks may be required.

- **Integration with internal billing service.** The WLAN infrastructure may be used for location-based services that are tied directly to the billing system of the venue. The OSS role is to facilitate the integration of the local Wi-Fi infrastructure with venue owner back-end systems, such as property management systems in hotels that enable services like on-line checkout.
- **Pricing flexibility.** If the venue owner gets a share of the revenues, it is keen on ensuring high traffic levels. Pricing flexibility is conducive to higher traffic levels as it more efficiently captures the potential demand among hotspot visitors. In particular, some venue owners may be interested in retaining the ability to market the service to visitors or to provide free access to customers (for instance through coupons that allow customers to have free WLAN access for a limited time).
- **Multiple virtual networks.** In some locations, the WLAN infrastructure may be used by the venue owner and its tenants for their own internal services, in addition to public access and location-based services. In this case, the network operator will be required to manage multiple virtual networks and to ensure that the traffic is kept separate for security reasons and to ensure that sufficient bandwidth is available to all users.

Network operator requirements: a robust and effective OSS to manage their WLAN infrastructure

Network operators occupy a central role in ensuring that WLAN is a carrier-grade service. They need to work with venue owners to ensure that they have their support and access to the facilities, and with aggregators, clearinghouses and service providers to ensure that the service runs smoothly. The responsibility for the network installation, maintenance, and operations mostly lies with the network operator. Service providers are instead responsible for billing, customer care and some provisioning functions. Requirements include:

- **Scalable and extensible system.** The OSS has to handle effectively any extension to a single hotspot's coverage area and any increases in the number of hotspots in the footprint.
- **Easy installation.** Installation of the WLAN infrastructure has to be streamlined and require a minimum of staff resources at the hotspot location.

- **Hardware independent network management.** An OSS that is not tied to specific hardware implementations and that provides multi-vendor hardware support will give network operators the necessary flexibility in selecting the hardware that is best suited to their needs.
- **Remote network management.** Expensive truck rolls may quickly become one of the major cost items in deploying and managing a WLAN. Remote network management allows the operator to keep operating costs associated with configuration, provisioning, and maintenance low.
- **Detailed traffic and usage monitoring.** Collection of detailed records allows service providers to offer multiple pricing options and network operators to effectively implement revenue sharing agreements. Once WLAN and cellular technologies become integrated, real-time billing may be needed by cellular carriers to prevent subscribers from exceeding their time or volume allocation.
- **Efficient use of the WLAN infrastructure.** In some instances, the WLAN infrastructure may be used by multiple networks (in the airport example at the beginning, for public access, security agency communications, airlines internal operations). This increases the utilization of the network deployed and may be conducive to higher revenues.
- **Robust AAA capabilities.** As the network operator deals with multiple aggregators, clearinghouses and service providers, it is important that it adopts a best practice AAA solution compatible with Remote Access Dial In User Service (RADIUS)[1]. In particular, secure authentication is necessary to gain the trust of service providers in implementing roaming agreements. Different service providers may prefer specific authentication methods (for instance, GSM and other cellular carriers may want to use the Extensible Authentication Protocol with the Subscriber Identity Module (EAP-SIM) authentication) and expect that their roaming partners support them.
- **Offer security to protect network and users.** Implementation of a robust security framework is necessary to protect the users and the network, and to gain trust of the other players. Network operators need to support security standards and solutions (Figure 3) that their roaming partners and the subscribers use.
- **QoS management.** Advanced services such as Voice over WLAN (VoWLAN) and high traffic levels require the introduction of QoS and load balancing to ensure an appropriate and efficient distribution of resources.

[1] In addition to RADIUS servers, solutions such as Microsoft's Active Directory and Sun's Identity Server offer RADIUS compatibility.

Service provider requirements: integrate the WLAN OSS into their legacy systems

Wi-Fi access is often offered as complementary to existing services: cellular carriers offer Wi-Fi access alongside voice and cellular data, broadband providers as an add-on to fixed broadband access, data service providers as a complement to dialup or fixed broadband access to the road warriors. As such, it is critical that the WLAN OSS can be easily and fully integrated with the existing OSS, both to improve the customer experience and to keep the costs down, by avoiding unnecessary duplication.

In addition, subscribers will often use Wi-Fi services in hotspots managed by roaming partners. The service provider will want to brand services at these locations and will need to have access to information about the network to provide effective customer support. This entails the exchange of information between network operator and service provider, possibly through an aggregator to coordinate these efforts.

Finally, Wi-Fi needs to be a carrier-grade service to successfully complement or compete with other cellular technologies and to allow service providers to generate revenues from it. To ensure that this is the case, an OSS needs to meet these service provider requirements:

- **Full roaming capability, with infrastructure supporting flexible wholesale contracts.** Roaming gives service providers access to a wider footprint, which in turn makes the service more attractive to subscribers. However, roaming may be an expensive service to offer (especially if roaming premiums are low or non-existent) as it requires the establishment and maintenance of several roaming partnerships. While aggregators and clearinghouses may help keep costs under control, a billing system that includes full support for roaming is necessary. The billing system needs to provide functionality to manage wholesale relationships with multiple roaming partners and clearinghouses (both for selling and buying access at a wholesale basis – i.e. providing access to subscribers from other networks and paying for the charges incurred by its own subscribers accessing the roaming partner's hotspots) and to bill subscribers.
- **Integration with existing billing and customer management systems.** As WLAN access will in most cases be a new, add-on service, it is typically more cost effective for service providers to integrate WLAN billing and customer care systems with the existing ones, than to switch to new ones. As a result, it is crucial that the OSS allows the service providers to

easily interface with established OSS for cellular and fixed operators and broadband providers.

- **Flexibility in setting multiple or tiered pricing options.** It is too early to know which pricing model will prevail and it is likely that different service providers will prefer different models. In all cases, they will want to keep their options open and be able to experiment and integrate Wi-Fi more or less tightly with other services offered. For instance, a cellular operator may want to allow subscribers to use their monthly minutes for Wi-Fi connections as well as voice. When QoS becomes available, tiered services may be linked to different pricing options.
- **Friendly and customizable end-user interface.** An easy-to-use, well-supported interface is crucial to reduce the burden and cost of customer support. Additional services such as online access to account management are desirable as they may further reduce costs.
- **Secure authentication and data transmission.** The OSS needs to offer secure connectivity to subscribers who require it and to allow other users to avail themselves of their preferred security solutions (e.g. VPN). In cases where the subscriber connects at a roaming partner's location, it is important that the user is authenticated directly against the service provider authentication servers and that the partner network operator does not have access to the subscriber authentication credentials. Providing secure connections will attract users (especially those who do not have VPN at their disposal) and constitute a differentiating factor from hotspots that offer free connectivity.
- **Branding of service.** Branding of the visited hotspot enables service providers to offer a consistent service, with a single interface and to add VAS that may increase subscriber retention and Average Revenue Per User (ARPU). As venue owners and franchises will also require to brand the service provided at their hotspot(s), branding information from different sources needs to be integrated in the splash page.
- **Access to information on roaming partners' networks.** While the service provider will not need extensive visibility into the partners' network, it will need to have sufficient information to provide customer support.

Key capabilities of an OSS that meets WLAN service requirements

A robust OSS for WLAN needs to offer a solution to the requirements identified in the previous section. We recommend that while evaluating different OSS options, service providers and network operators focus on four dimensions:

- **Ability to manage increasing complexity.** The OSS needs to offer the flexibility, extensibility and scalability required to manage an increasingly complex footprint and the subscriber base demands for advanced functionality. The OSS needs to be developed with an eye towards advanced services and must facilitate the introduction of new services.
- **Support for standards and widely adopted solutions** (e.g. WPA and VPN for security, RADIUS for AAA, or billing formats such as Internet Protocol Detail Record (IPDR), Transferred Account Procedure (TAP), Cellular Intercarrier Billing and Exchange Roaming Record (CIBER) and, in the future, Mobile Xchange Protocol (MXP)) (Figure 4). A standard-based OSS is crucial to ensure interoperability with roaming partners, to facilitate integration with existing billing and customer management systems, and to meet the security and usability requirements of subscribers and corporate accounts managers.
- **Offer an easy-to-use, effective, and consistent interface to the user.** Users need to rely on an interface that is straightforward to use, without assuming any knowledge of the operations of the underlying technology. Furthermore, it must enable them to monitor and manage their accounts online.
- **Provide a cost effective solution.** The OSS should allow service providers to avoid duplication of OSS functionality (e.g. in billing and customer care) and to streamline the deployment and management of the OSS infrastructure.

IPDR	IPDR NDM-U (Network Data Management - Usage) protocol has been specifically developed for IP services, both for wired and wireless services.
TAP	Billing protocol used by GSM mobile operators.
CIBER	Billing protocol used by IS/ANSI41(TDMA and CDMA) mobile operators.
MXP	XML-based billing protocol introduced by CIBERNET to support data VAS.
RADIUS	RADIUS is the AAA protocol that provides the data to be converted into IPDR, TAP, CIBER and MXP.

Figure 4. Billing protocols for WLAN services

A look at the future

Selection of an OSS needs to be made with reference to the future developments of the service, as its adoption and integration with legacy systems requires a substantial initial effort. WLAN services have not yet reached maturity and they are rapidly evolving. Currently, Internet access is the dominant service offered, on a best-efforts basis. Over-the-air security is not yet commonly offered and location-based services are still in their infancy. In these circumstances it is difficult to predict the evolution path for WLAN services and the OSS requirements that they will introduce. Some trends however can be discerned, along with key functionality that will be increasingly expected from the OSS.

One question that remains open is which of the advanced VAS (gaming, VoWLAN, etc) will be offered by the WLAN value chain players, namely the service provider, network operator and venue owners, and which ones will be offered by the same companies that offer those services on the Internet for free or for a fee (e.g. Skype, iTunes, or New York Times). Once the subscriber is connected, services from online providers are readily available and, if WLAN services offered by the service provider are not competitively priced, online providers may easily retain or capture this market.

Location-based services. Today subscribers gain access to a WLAN through a web-based interface that typically carries information about the service provider and in some cases about the hotspot. Venue owners see the opportunity to provide local services and information about their venue and to charge for some of these services. Nearby venue owners may be interested in placing ads promoting their business in the WLAN web interface. Users can already do at least one type of transaction at the hotspot without an existing subscription: sign up for service or pay for the access during a restricted period of time. In the future, it is likely that the range of WLAN-based transactions and the amount of local information available will widen, thus increasing the importance of an effective communication channel among venue owners (pushing for most local services), network operators and service providers. If services are billed to the subscriber account, the OSS has to offer the functionality to process micro-payments.

VoWLAN. VoIP is making quick progress in the enterprise and in the fixed telecommunications markets in North America, and VoWLAN is one of the hot applications for WLANs in the enterprise. The public hotspot market is not yet ready for VoWLAN, both because the devices are not yet for sale (although several manufacturers are working on handsets using 802.11b) and because QoS is necessary, but no standards-based solution is yet available. IEEE 802.11e, when ratified, will provide support for QoS and will facilitate adoption of VoWLAN. It is still uncertain whether cellular carriers will want to use the WLAN infrastructure to route voice calls when subscribers are in hotspots: while WLAN may provide a cheaper over-the-air link and it may help relieve congestion in the cellular network, coexistence of cellular voice service with VoWLAN makes service provisioning more complex. It is also possible that other service providers, such as WISPs, may elect to offer VoWLAN for free, with the user simply paying for access charges, as voice effectively becomes an additional data service which is inexpensive to provide.

Online gaming. While the predominant applications for WLAN public access over the next few years will still be email, web surfing and Internet connectivity, online gaming is one of the most interesting emerging applications, as it is targeted at the consumer users, a segment that will grow quickly once WLAN becomes more widely embedded in laptops and PDAs. Games have proven to be a successful application for cellular devices; WLAN higher bandwidth and the possibility to establish peer to peer connections make online gaming is a likely winner. It is not yet clear however, how a WLAN service provider can generate revenues from it, other than from the increase in traffic that gaming may generate. Gaming will put additional requirements on the WLAN infrastructure, as it will require a close monitoring of performance and possibly the introduction of QoS. Support for micro-payments will also be necessary if revenues are to be extracted from downloading or playing games.

Content downloads and streaming. Today subscribers can already download content and stream video or audio, either for free or by paying the content providers directly. Because traffic on WLANs is still on average below capacity, downloads do not cause problems. In an environment where usage is high, it may be necessary to use QoS, load balancing and more sophisticated network management tools. In addition, specific types of content (e.g. music, films) may require a micro-payment from the user and specific tools for digital rights management.

Interworking with other wireless technologies. While not yet in demand, interworking with other wireless technologies, including cellular networks, IEEE 802.16 (WiMAX) and IEEE 802.20, will become a requirement within a few years. While today's users typically access a WLAN from a laptop, an increasing share of traffic will come from PDAs, phones and other mobile devices. The increased mobility that these devices promote will make interworking with other wireless technologies more useful, as users will often walk or drive beyond the WLAN area of coverage.

Pronto Networks' OSS solution

Pronto Networks has developed Pronto Hotspot OSS to address network operators' and service providers' requirements for a carrier-grade service. Pronto Hotspot OSS is a modular, scalable platform that enables the provisioning, management and deployment of large and small public Wi-Fi networks. Pronto's solution is based on industry standards, such as 802.1x, WPA, Protected EAP (PEAP), and supports VPN, WPS, as well as multi-vendor hardware. It has been designed using Pronto's experience in providing Wi-Fi managed services to hotspot operators and service providers, using Java 2 Enterprise Edition (J2EE) technology. Pronto's platform is well suited to network operators and service providers that need to work together with a wide range of roaming partners and need to integrate WLAN services with their existing product offerings. Figure 5 shows the key capabilities and benefits of Pronto Hotspot OSS.

Billing	Customer Management	Network Management	Service Provisioning	Service Assurance
Support for multiple authentication credential types Flexible pricing, rating and discounting of usage based and flat rates Multiple payment options, including credit cards, invoices, and pre-paid cards. Configurable online bill formats Integration to third party billing systems via IPDR Integrated billing, clearing and settlement	Customer self-care portal Credit limit management Incident tracking Account adjustment and returns Service provider branding	Bandwidth management capabilities Management and remote upgrades on edge elements SNMP support Location-specific content and interface Real time system administration and configuration ability Automatic email alerts Easy integration with external NMS products Support for SOAP, 802.1x, RADIUS, VPN, SSL encryption, and EAP methods	Web-based service management Service creation with QoS Provisioning of Pronto and third party gateways Support for iPass, GRIC and Boingo clients	Monitoring of edge elements Real-time reports and statistics

Figure 5. Pronto Hotspot OSS

Final recommendations

As WLAN services become more widely available and popular, the requirements for service providers, network operators and intermediaries, such as clearinghouses and aggregators, are becoming better defined and more stringent. Managing the WLAN infrastructure is becoming more demanding, because of the growing number of hotspots and their more complex architecture (wider coverage, multiple networks, support for roaming and security). The increasing availability of roaming and the need to provide a carrier-class service that can be integrated with existing ones poses new challenges for service providers and intermediaries alike.

The availability of standards like 802.1x and WPA for authentication and security, IPDR, TAP and CIBER for billing information, and of widely used solutions like RADIUS for AAA, or VPN for security makes it possible to have a robust infrastructure that enables service providers to offer WLAN as a carrier-grade service. However, to achieve this goal, network operators and service providers need to carefully evaluate the OSS solutions available and ensure that they meet the requirements for WLAN access. This paper identifies requirements that need to be satisfied to ensure that the subscribers receive a compelling service and that all the value chain players can work together toward this goal.

The initial challenge for WLAN service providers was to be able to offer connectivity across a sufficiently wide footprint. The rapid growth in the number of hotspots and the progress toward establishing a wider network of roaming agreements show that service providers and network operators are moving in the right direction. The next challenge is to ensure that the infrastructure deployed can be used to offer a service that users will find attractive and easy to use, while being cost effective for network operators and service providers. The adoption of robust, yet flexible OSS will be crucial to meet this challenge.

About Senza Fili Consulting LLC

Senza Fili Consulting (www.senza-fili.com) provides advisory support in wireless data technologies and services, including Wi-Fi, cellular, satellite, and wireless broadband. Founded in July 2003, at Senza Fili we have in-depth expertise in financial modeling, market forecasts and research, white paper preparation, business plan support, due diligence, and evaluation of end-user interface requirements. Clients include service providers, manufacturers, and developers of solutions for wireless technologies.

Monica Paolini is the founder of Senza Fili Consulting. She is an expert in wireless technologies and has helped clients worldwide to understand technology and customer requirements, evaluate business plan opportunities, market their services, and estimate the market size and revenue opportunity of specific services. She has frequently been invited to give presentations at conferences, has written several reports and white papers, and her work on Wi-Fi is often quoted in the press. She can be contacted at monica.paolini@senza-fili.com.

About Pronto Networks, Inc.

Pronto Networks is a privately-held company offering carrier-class Operations Support Systems (OSS) that enable network operators to provision, manage and deploy large scale public WLAN networks. Pronto's OSS handles provisioning, configuration, authentication, access control, security, pre-paid and post-paid billing, and roaming settlement for large public WLAN networks, in addition to remotely managing and updating multi-vendor hardware and Wi-Fi switches. Pronto's OSS is modular, multi-tier, and highly scalable, and offers a pluggable architecture for enabling or disabling system components. The OSS is built on new generation technologies based on J2EE and utilizes SOAP and Webservices for integration into third party systems and the creation of new value added services.

Pronto's OSS is being used in the provisioning, management and deployment of thousands of Wi-Fi hot spot nodes worldwide. Pronto's OSS supports a variety of locations including airports, hotels, convention centers, restaurants, multi-dwelling units, marinas, and truck stops.

Pronto Networks is funded by Draper Fisher Jurvetson and Intel Capital. In 2003, Pronto Networks has received several awards including Wired Magazine's Top 25 Wi-Fi Companies to Watch, the AlwaysOn list of Top 100 Private Companies, and Computerworld's Innovative Technology Awards.

For more information about Pronto Networks, please contact:

Pronto Networks
Corporate Headquarters
4637 Chabot Drive, Suite 35
Pleasanton, CA 94588
925 227 5500
www.prontonetworks.com
info@prontonetworks.com

This white paper was commissioned by Pronto Networks, Inc. Pronto Networks retains the right to redistribute the integral version of this report. No selection of this material can be copied, photocopied, duplicated in any form or by any means, or redistributed without express written permission from Senza Fili Consulting LLC. While the white paper is based upon information that we consider accurate and reliable, Senza Fili Consulting LLC makes no warranty, express or implied, as to the accuracy of the information in this document. Senza Fili Consulting assumes no liability for any damage or loss arising from reliance on this information. Names of companies and products here mentioned may be the trademarks of their respective owners.