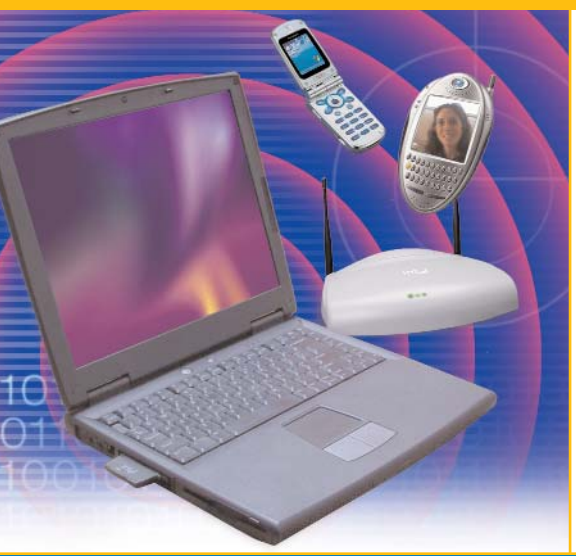
Volume 07 Issue 03 Published, August 19, 2003 ISSN 1535-864X



# Intel® Technology Journal

## Wireless Technologies

# Public WLAN Hotspot Deployment and Interworking

A compiled version of all papers from this issue of the Intel Technology Journal can be found at:
http://developer.intel.com/technology/itj/index.htm

# Public WLAN Hotspot Deployment and Interworking

Prakash Iyer, Corporate Technology Group, Intel Corporation
Victor Lortz, Corporate Technology Group, Intel Corporation
Lee Tapper, Corporate Technology Group, Intel Corporation
Roger Chandler, Corporate Technology Group, Intel Corporation
Roxanne Gryder, Corporate Technology Group, Intel Corporation

Index words: WLAN, 802.11, Wi-Fi, Roaming, Hotspot, WPA

## ABSTRACT

Wireless data networking is becoming more and more popular, and network operators of various kinds (cellular providers, wireless Internet Service Providers, etc.) are beginning to deploy public Wireless Local Area Network (WLAN) hotspots around the world. However, broad adoption of these hotspots may be inhibited by technical obstacles such as ease of use, security, and the inability of users to roam across hotspots as they can with cell phones today. The latter problem in particular highlights the need for a common hotspot architecture that is based on open standards and is acceptable to different service provider communities. Such an architecture must also be flexible to accommodate users with a variety of mobile device form factors and login credential types, as well as different billing models.

We begin with a brief survey of the state and deployment of hotspots today and go on to describe a unified public hotspot architecture that addresses the technical obstacles mentioned above. A major theme of the paper is the transition from the insecure Universal Access Method (UAM) to more robust authentication and link security based on Wi-Fi* Protected Access (WPA*). While much of the discussion centers on authentication and authorization for internet access, we also touch upon issues that need to be addressed to enable more advanced services to be deployed and accessed from such hotspots in the future.

## INTRODUCTION

Deployment of public Wireless Local Area Network (WLAN) hotspots, initiated by a diverse set of incumbent operators—cellular carriers (GSM and CDMA), Wireless Internet Service Providers (WISP), dial-up aggregators, and fixed broadband operators (xDSL, cable)—is growing rapidly across the globe. The predicted rate of deployment of WLAN technologies is impressive. The analyst firm Gartner predicts that by the year 2008 there will be more than 167 thousand public WLAN hotspots around the globe. In addition, there will be over 75 million users of public WLAN hotspots worldwide [1].

While the outlook for WLANs appears to be promising, there are several factors that may limit their viability as effective global solutions for wireless data connectivity. The following observations are worth noting:

- Each operator/carrier community has its own business models and independent standards' forums that are enabling "WLAN roaming and interworking" scoped primarily for that community.
- Hotspot deployment in urban areas is unlikely to be monopolized by individual operators or operator communities—limiting the available footprint for users—unless a common roaming framework is deployed. Therefore, intra-city roaming for WLAN users will be required if providers are to expand the use of their hotspots. Moreover, hotspot deployment has great potential for revenue generation, *a la* roaming in the cellular world.
- The smaller cell sizes, the low cost of equipment, and the lack of regulatory barriers for WLAN deployment encourage a greater diversity of operators to enter the business. Consequently, roaming will likely become more common for public WLAN users than for cellular users.
- With technology evolving rapidly, there is a substantial risk of fragmentation from this early

*Other brands and names are the property of their respective owners.

deployment of hotspots, thus inhibiting regional and global interoperability.

- User adoption may be slow if public WLAN services are not cost effective, widely available, secure, and easy to use.

These observations highlight the need to establish a common hotspot architecture that all operator types can embrace. In the remainder of this paper we describe a conceptual blueprint for hotspots, discuss authentication and security issues, and consider billing and settlement architectures to enable worldwide one-bill roaming for public WLAN.

## THE PROPOSED HOTSPOT BLUEPRINT

Figure 1 is a conceptual illustration of a common hotspot blueprint that shows how a single hotspot could support roaming users with accounts managed by a wide variety of home operator types. For this approach to be practical, the authentication mechanisms and Authentication, Authorization, and Accounting (AAA) signaling between the hotspot and the different back-end authentication systems of different operator types must be compatible.

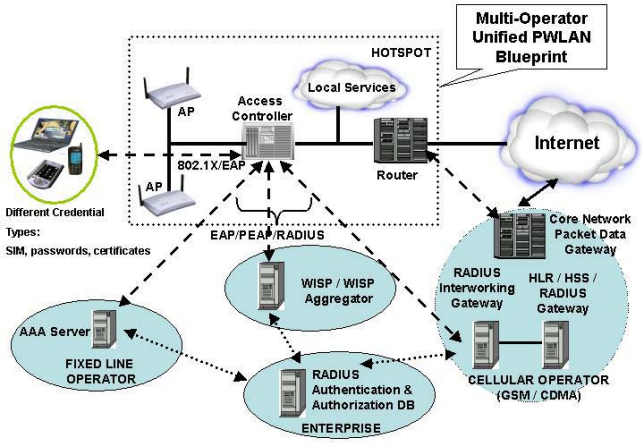



**Figure 1: Conceptual hotspot blueprint**

If a consistent approach for hotspot authentication, accounting, and billing can be established in the industry, it will become much easier for home operators of various types to begin offering public WLAN service to their customers. Home providers do not need to provide wireless network services in this model. All the home provider needs to do is to deploy AAA and billing infrastructure and to establish roaming agreements with one or more WLAN operators.

### The State of WLAN Deployment Today

While the global proliferation of Wireless Local Area Networks (WLANs) continues at a rapid pace, the methods by which these networks are deployed—particularly in the public domain—are diverse and somewhat chaotic. According to the Wi-Fi Alliance[1], the most prevalent form of access today is based on web-browser hijacking and is referred to as the Universal Access Method (UAM). With browser hijacking, the hotspot redirects the user's browser to a local web server secured by TLS [2] (the standard security mechanism for web pages). The user's identity is authenticated to the UAM login page by entering a username and password on a form sent to the web server. Significant advantages of this method are ease of deployment and the fact that mobile clients need only support a web browser to gain access to a hotspot.

Although UAM is simple and easily deployed, it has several serious drawbacks. One problem is the user experience. Research shows that the first step to obtain network access, i.e., launching the browser, is not intuitive if the intent is to use some other application such as an e-mail client. Furthermore, enterprise users frequently require Virtual Private Network (VPN) policy settings that conflict with the requirement to access a local web server. More seriously, however, UAM typically exposes the user's credentials (username, password) to the visited network's web server—an unacceptable feature for carriers that do not wish to expose subscriber databases, even to legitimate roaming partners. Furthermore, unless the user manually inspects the certificate used by the server to secure the web pages (which is rarely done), these credentials may be unwittingly disclosed to an attacker operating a rogue wireless access point (AP).

Most of the security problems of UAM can be overcome by using Wi-Fi Protected Access, also called WPA [3]. WPA uses IEEE 802.1X [4] authentication to mutually authenticate the AP and mobile client. It also uses the Temporal Key Integrity Protocol (TKIP) to encrypt packets and prevent forgeries. The use of WPA and the seamless transition from UAM to WPA are major themes of this paper.

There are also several inconsistencies in the end-to-end architectures of currently deployed hotspots that are often caused by the variety of AAA backends of the incumbent operators. For example, broadband carriers typically use RADIUS servers natively, while Global System for Mobile Telecommunications (GSM) cellular carriers interface to SS7[2]-based backends. In a rush to offer richer, more enhanced services, service providers have also deployed a variety of proprietary systems that require

[1] http://www.wi-fi.org/OpenSection/index.asp

[2] System Signalling No. 7 is an ITU-T telecommunications standard.

complex software configurations on mobile clients. This is clearly an impediment to ease of use and ubiquitous access. Another source of inconsistency from the user's perspective is that WLAN service is sometimes provided for free. Users accustomed to free service may be confused when they discover that in a different venue they are expected to pay for service.

## Tenets for a Unified Architecture

The unified hotspot architecture proposed in this paper is based on the following requirements and architectural principles:

- WLAN hotspots are essentially 802.11-based IP networks and, as such, we strongly subscribe to the use of core protocols developed in the IEEE (such as 802.1X) and the Internet Engineering Task Force (IETF). This minimizes the need for proprietary or domain-specific protocols to be used over the WLAN interface.
- The hotspot must support a common user sign-on experience that is independent of or agnostic to variations in network backends.
- The core components and interfaces of the blueprint must be agnostic to the type of hotspot operator (e.g., Wireless ISP (WISP), DSL provider, cable modem provider, or cellular operator).
- The visited hotspot must accommodate a variety of credential types (e.g., username/password, Subscriber Identity Module (SIM), and X.509 certificates) and enable new forms to be introduced over time.
- In a subscription-based access model, it must be possible to provide end-to-end security for authentication and authorization; i.e., users should be able to securely and bilaterally authenticate with the subscription home provider. The home provider should prove its identity first, before any user-specific identity is divulged, and true identities should only be exposed to the home provider.
- It must be possible for different users to avail of different levels of service depending on whether they are in the home provider's network or in a visited network.
- The framework must accommodate older UAM authentication models while articulating a clear strategy for interim coexistence and longer-term migration to more robust schemes, based on 802.1X.
- If possible, key distribution between home providers and visited networks for wireless link layer encryption should be secured and cryptographically bound to authentication and session information. (*Current* standards for WLAN key distribution do not fully meet this requirement in roaming scenarios.)
- Reauthentication when moving between access points (APs) managed by the same network operator must not cause significant delay and must not require user interaction.
- If protocol translations are required to be integrated with legacy or proprietary authentication backends, such translations should occur within the premises (architecturally speaking) of the legacy network.
- In situations where integration of services requires interworking with another network (such as a cellular operator's core data network), we advocate the notion of "loose coupling" between the WLAN hotspot and core networks. In other words, WLAN networks should be seen as standalone networks based on IEEE and IETF core protocols as opposed to radio access networks, and should not require the use of domain-specific mobility management protocols over the client's WLAN interface (for example, GPRS Mobility Management or GMM). This philosophy is also in line with a future vision where all wireless networks will be natively based on IETF's suite of IP protocols.

## Generic Public WLAN Roaming Model

Figure 2 depicts a generic architecture corresponding to the hotspot blueprint for public Wireless Local Area Network (WLAN) roaming. Real-world roaming scenarios can encompass a large number of possible scenarios and network configurations. To make this complexity manageable, we define a generic roaming model that ignores non-essential aspects of roaming. For example, although a home provider may often operate a hotspot, the essential characteristic of the home provider in our model is that it maintains the user/subscriber relationship and implements an Authentication, Authorization, and Accounting (AAA) service to authenticate roaming users. Home providers do not need to provide wireless network services to fulfill this role.

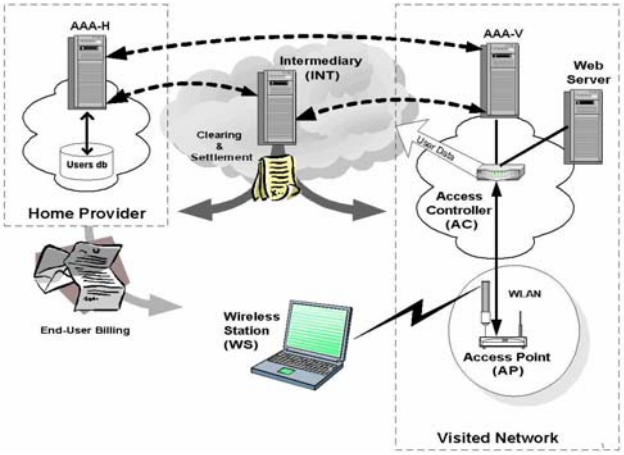



**Figure 2: Generic roaming model**

There are seven primary components in the generic roaming architecture:

1. The *Wireless Station (WS)* represents the user's equipment (typically a laptop computer, cell phone, or PDA) that is used to access the 802.11 network.
2. The 802.11 *Access Point (AP)* terminates the air (radio) interface to and from the WS.
3. The *Access Controller (AC)* is the entity that verifies authorization and enforces access control for authenticated users and segregates traffic of non-authenticated (guest) users.
4. The *Visited Network AAA Server (AAA-V)* serves as an AAA proxy for roaming (foreign) customers.
5. The *Home Provider AAA Server (AAA-H)* serves as the RADIUS server authenticating the WS user. The home provider and visited network operator AAA servers also participate in transactions involving the reconciliation of billing and settlement records—both online and offline—and either mutually, or via an intermediate settlement entity.
6. The *Web Server* is an optional component that could serve one or more of the following functions: browser-based login portal, local value-added services portal for guests and authenticated users, portal for new subscriptions, and redirector for other services.
7. The *Roaming Intermediary (INT)* represents a wide variety of AAA and billing intermediaries. Such functions might include AAA aggregation, wholesale hotspot service aggregation, AAA brokers and charging, billing and settlement clearing houses. They are typically implemented across multiple physical components.

It is important to note that these components are logical entities rather than literal components.

Figure 2 conceptually depicts only one possible billing model, where the home provider delivers a bill to the user. Equally valid are models where billing reconciliation is between an intermediary and the home provider or between the intermediary or visited network and the home provider.

## AUTHENTICATION AND SECURITY

One of the biggest barriers to WLAN deployment is security. It is important to understand that the threats associated with network impersonation on Wireless Local Area Networks (WLAN) is substantially worse than with most other networks. With wired networks, the user's direct connection to the network has at least some level of implied authenticity by virtue of physical wires or use of virtual circuits (e.g., ATM virtual circuits) or physical circuits (e.g., dial-up). In a WLAN, there is no such first line of defense. Unless robust mechanisms to authenticate the network are employed, the user is highly vulnerable to man-in-the-middle or rogue access point (AP) attacks on the wireless link.

The sensitivity and the value of data stored on many WLAN client devices such as laptops, and the high bandwidth of WLANs offer a significant incentive to attackers. A rogue AP, since it has complete control over the channel of information flow, can perform a wide variety of attacks including eavesdropping, message insertion, message modification, Domain Name System (DNS)-based attacks, etc. Link-level encryption does not protect against this class of attacks if the attacker is one of the endpoints of the encrypted channel.

There are two basic strategies to defend against rogue AP attacks. One is to tunnel all traffic through the rogue AP using a Virtual Private Network (VPN) client and a client-hosted firewall. If executed properly, this defense limits the rogue AP to denial-of-service attacks. However, the VPN approach requires a VPN infrastructure in the network and on the client, plus robust configuration of the client firewall. These are non-trivial requirements. An alternative strategy is for the client to authenticate the network and refuse to connect to a rogue AP. Note that the latter approach is only effective if subsequent use of the connection is cryptographically bound to the authentication.

### Wi-Fi Protected Access (WPA)

The security solution defined for the initial 802.11 standard called Wired Equivalent Privacy (WEP) had

several documented vulnerabilities, inhibiting its use and prompting the use of UAM with VPN. The IEEE 802.11 Task Group i (TGi) has addressed these weaknesses in the new standard branded by the Wi-Fi Alliance as WPA. WPA is based on the IEEE 802.1X authentication framework, but it improves on WEP by using dynamic per-user encryption keys and per-message integrity protection. TKIP, which is used by WPA, also constructs a new per-packet encryption key in a way that defeats the Fluhrer-Mantin-Shamir attack on WEP. WPA will be eventually superceded by a TGi specification that will essentially include support for the Advanced Encryption Standard (AES) and solutions for inter-AP roaming.

With 802.1X, the WS can initially access only the unauthenticated port on the AP (or network switch behind the AP, depending on the implementation). The unauthenticated port typically limits the WS to using the Extensible Authentication Protocol (EAP) [5] protocol and communicating with the network's authentication infrastructure. If the WS and network successfully authenticate and satisfy each other's access control requirements, the session key derived by the WS is granted access to the authenticated port. The corresponding key for the WLAN network infrastructure is also communicated by the AAA-H to the AP. At this point, the WS is typically given access to the Internet.

Figure 3 depicts a typical protocol stack for WPA-based authentication. The framework permits an AP to block all unauthenticated traffic from accessing the Internet or other service networks, until the mobile client is authenticated by a provider—the visited network in prepaid or pay-for-use billing models and the home provider in subscription-based billing models.

The WPA framework relies on the EAP as the framework to carry protocol messages between the supplicant (client), authenticator (AP), and authentication server. The EAP messages are carried over EAPOL (EAP over LAN) frames between the WS and the AP and reencapsulated in RADIUS messages from the AP to the home AAA server (via zero or more AAA proxies). For security reasons, RADIUS is sometimes also carried over IPsec. In future, RADIUS may be natively substituted by DIAMETER, a successor AAA protocol being developed by the IETF.

The WPA/802.1X model offers significant advantages over the browser hijack model. One of the most important advantages is that 802.1X is designed to support extensible end-to-end authentication between the WS and the home provider's AAA-H.

The EAP channel established by 802.1X can support a variety of authentication protocols and credential types—all that is needed is an EAP method with appropriate security properties describing how the protocol is encapsulated by EAP. The EAP method must (a) perform mutual authentication, (b) derive fresh session keys, (c) be immune to man-in-the-middle attacks, and (d) be immune to dictionary attacks.

When the EAP channel is established between the WS and the AAA-H, there is no need for the visited network's AP, AC, or AAA-V to comprehend or support the specific EAP method or credential types used by the home provider. This feature provides great flexibility to the client and service providers.

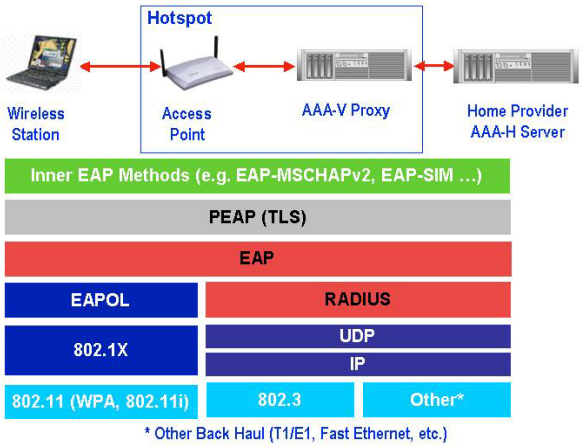



**Figure 3: 802.1X/WPA with PEAP**

To achieve end-to-end identity confidentiality, it is recommended that the Protected EAP [6] tunneling authentication protocol be used. PEAP is an authentication tunneling protocol that creates a protected channel for other EAP-based authentication methods. PEAP enables two-phase mutual authentication where the network first authenticates to the client via a digital certificate and then the client authenticates to the network using some other EAP method inside an encrypted channel. The client authentication method is typically based on passwords rather than client certificates. This is the same model used by secure web sites; however, the use of domain-specific root certificates with PEAP greatly improves the trust model over the more traditional browser used by e-commerce. This is because the large number of commercial root certificate authorities trusted by browsers has a business incentive to issue as many certificates as possible, and it is relatively easy for an attacker to obtain such a certificate.

With PEAP, common session key derivation, distribution, and configuration solutions can be defined for a variety of credential types, including certificates, username and password, and Universal Subscriber Identity Modules USIM. If industry alignment can be achieved in these areas, it will be easier for network operators to support a variety of roaming scenarios across different network

types. PEAP helps address the user security requirements in the 3GPP Release 6 TR 22.934 document. Furthermore, the TLS and the PKI infrastructures used by PEAP can also help address many of the requirements for network operator security features listed in TR 22.934. Alternatives such as Tunneled TLS [7], which has similar functionality, can also be used without significantly sacrificing interoperability, because of the end-to-end properties of EAP. However, PEAP is likely to be more widely deployed on client platforms due to native operating system integration.

A new version of PEAP is being developed that includes a fix for man-in-the-middle attacks that are possible when the same credentials are used both inside and outside of PEAP. When this version of PEAP becomes available, we recommend only using it with inner EAP methods that can derive keys. In the case of passwords, this would imply the use of EAP-MSCHAPv2 over legacy methods such as EAP-OTP, EAP-MD5, or EAP-GTC. Also, while PEAP may seem redundant when used with EAP methods that inherently offer bilateral authentication and 128+ bit key derivation (like EAP-AKA with USIM cards), PEAP has a property called session reuse that can optimize handoffs across APs.

## IP and MAC Address Filtering

A common method for controlling internet access for WLAN networks is to filter packets based on the source IP address and/or MAC address. This method can be used to limit a WS access to only designated destination addresses such as the browser hijack web server. Although this is a very common method for access control, in many cases proprietary implementation methods are used. This is an area where additional standardization work may be needed.

## VLAN Support

Virtual LAN (VLAN) technology can provide additional flexibility to the deployment of WLANs, because it can be used to provide logical isolation of traffic sent through common WLAN APs. This can be used to enhance the security of portions of the traffic to support more robust billing methods, enable infrastructure sharing among carriers, and to separate private WLAN connections from public access traffic. For example, broadcasts directed to secure network segments are encrypted and thus protected from weakly authenticated users, if the traffic is separated. In 802.11, there are no physical VLAN ports, so VLAN membership is often assigned dynamically as part of the authentication process via RADIUS accept messages. Another possibility is to assign VLANs one-to-one with 802.11 Service Set Identifiers (SSIDs). VLANs can also provide a mechanism for associating users with site-to-site tunnels used to direct data traffic to the core networks of roaming partners. VLANs can be used in conjunction with IP and MAC address filtering to control what parts of the network are available to specific WSs.

## Migration to WPA

Although we prefer 802.1X and WPA, we also recognize that until 802.1X-capable clients are widely deployed, there will be a market requirement to support the Universal Access Method (UAM). Furthermore, even when 802.1X is used, browser hijacking can be useful to help resolve authentication failures and to permit the establishment of new accounts. Therefore, the generic hotspot architecture supports a mixture of UAM and 802.1X-based authentication.

Figure 4 illustrates a possible coexistence strategy involving the use of a VLAN-capable AP to separate UAM traffic from 802.1X traffic. To support both 802.1X and UAM, each AP supports two different Service Set Identifiers (SSIDs), one corresponding to 802.1X and one open (for UAM). With current AP hardware, only one of these SSIDs would be advertised by the AP (corresponding to WPA), but the other (for UAM) could be discovered via the 802.11 probe request/response mechanism. The open SSID would not require any link-layer security, but the AC would limit user access to the local web server until the user obtains authorization to use the network. Subsequent enforcement of access control for the UAM method is likely to be based on the client's MAC address, which is not very robust. Attackers can easily configure their own equipment with the same MAC address and masquerade as legitimate users, stealing their bandwidth. This creates a business incentive for network providers to migrate users away from the UAM as soon as possible.

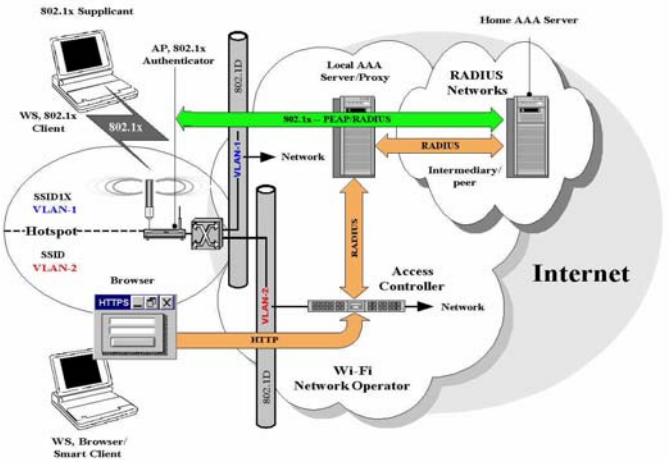



**Figure 4: 802.1X and UAM/browser hijack coexistence**

If an AP is capable of advertising multiple SSIDs, the WS will be able to detect them and choose the appropriate one. If the AP can only broadcast one SSID, the WS may be able to probe for the hidden one by using a database of hidden SSIDs. Since such preconfiguration is not practical when roaming, the industry needs to develop better ways to discover hidden 802.11 SSIDs.

The AP assigns separate VLAN tags to packets according to the SSID the WS is associated with. The VLAN switch in turn routes the packets during authentication so that the 1X traffic gets sent to the AAA-V for authentication, and the browser hijack mechanism is used for the non-1X clients. The web server for the browser hijack is not shown in the figure (it could be implemented by the access controller). Note also that although the figure does not show the access controller in the data path for the 1X traffic, in many implementations it will be.

Other coexistence models are possible as well. For example, if traffic from the 802.1X clients and browser hijack clients is mixed, the VLAN switch can be eliminated, and the Access Controller can manage both types of clients. However, this approach is not as secure as the approach shown in Figure 4.

## ARCHITECTURAL CONSIDERATIONS FOR ONE-BILL ROAMING

Users of hotspot services could participate in one of several billing models; prepaid, pay-for-use, and postpaid (subscription-based) are likely to be the most common. Furthermore, charging itself could be based on fixed or flat rates, based on usage (time, bytes and/or number of connections) and services used. Regardless of the billing model, roaming users should have the same experience when connecting to a visited network as they do when connecting to their home network. Ideally, charges associated with WLAN roaming usage would appear in an integrated single bill as is the case for cellular voice roaming today.

Prepaid and pay-for-use settlement procedures are often localized to the visited operator or managed by a clearing house on behalf of the visited operator. Postpaid billing, on the other hand, requires business agreements between the visited and home operators. The simplest scenario is one in which each operator executes a bilateral agreement with every peer roaming partner. In the world of public WLANs, this may not be appropriate for two reasons:

- The number of service providers will be very large, creating a scalability problem.
- Since incumbent operator communities subscribe to different billing and settlement practices, there may be incompatibilities.

This is where clearing houses can play a role. Figure 5 conceptually depicts a Data Clearing House (DCH) serving the role of a settlement intermediary. The DCH connects via a chain of RADIUS/AAA proxy intermediaries to one or more hotspots and transacts charging, rating, billing, and settlement with diverse backends, using protocols such as RADIUS, TAP, CIBER, IPDR, and others. DCHs specialize in being able to convert different record formats to one format and in providing other value-added services such as re-rating and fraud detection.

For example, different versions of TAP may be supported by the billing subsystems of different home providers. A DCH can do the necessary conversions so that accounting or charging records originating from a visited WLAN can be processed correctly by a given home provider.

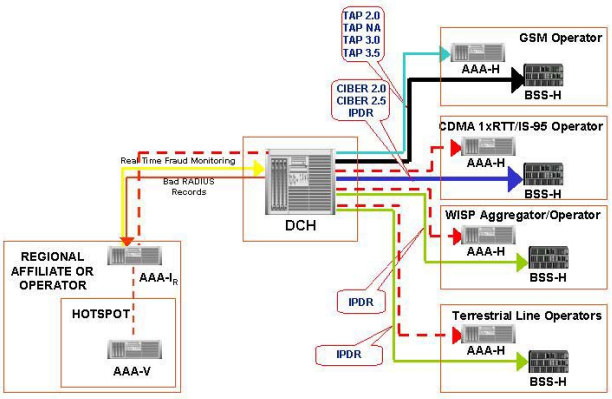



**Figure 5: WLAN Inter-operator postpaid settlement**

For one-bill roaming to work on a global scale, we propose a two-tiered model as depicted in Figure 6 below. This notion of a backbone of roaming intermediaries (only one DCH is shown in the figure for simplification) results in better scaling of roaming agreements and RADIUS traffic aggregation. Such a system can also combine prepaid and postpaid billing models.

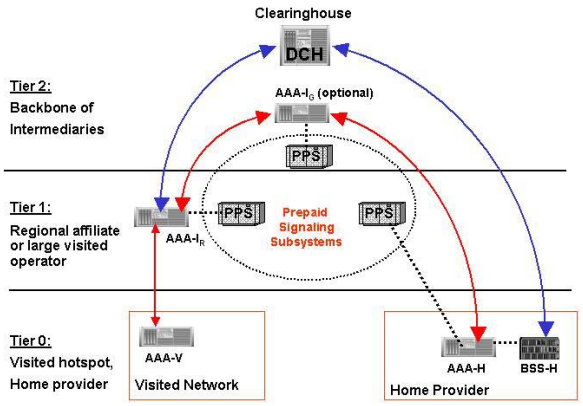



**Figure 6: Two-tier model for billing and settlement**

The idea of using regional affiliates in conjunction with global clearing houses has proven to be an effective model for billing and settlement scalability in the cellular industry.

## THE ROAD AHEAD

Future research will focus on the following areas as this architecture continues to evolve to support more advanced usage models:

- *Fast and seamless inter-access point (AP) handoffs*: The next big step is the introduction of value-added services to public hotspots that will include messaging, real-time multimedia streaming, and data application portals. These services require fast and lossless handovers across APs. The suite of solutions include improvements in TGi for pre-authentication and fast reauthentication, early Protected EAP (PEAP) termination and PEAP session resumption, as well as secure context transfers across APs
- *Wireless wide area network (WWAN) interworking*: Authorization and access to IP data services in GSM and CDMA core networks (2.5G and beyond) from WLAN hotspots will require solutions such as mobile IP overlay over GPRS for IP session persistence across WWAN and WLAN, the use of tunneling to ensure IP address reachability, and enabling of access to native IPv6 services like IP multimedia subsystems (IMS) over heterogeneous IPv4-IPv6 clouds. There are also significant challenges inherent in services provisioning and authorization, given the diverse set of operator types.
- *Public key-based authentication and authorization*: The use of public key-based authentication with attributes for dynamic services provisioning and authorization will overcome cryptographic limitations with use of passwords, not require use of expensive legacy token schemes like Generic Token Card (GTC) and SIM, and promote a more homogeneous framework for network access, whether in the home, enterprise, or public hotspots.
- *Network and services discovery*: There is a need to create a common yet extensible standardized framework for hotspot discovery, selection of service providers, and provisioning and use of services.

## SUMMARY

In this paper, we examined a variety of issues related to public Wireless Local Area Network (WLAN) roaming. Although there is substantial interest in developing a global WLAN roaming market, unless the technical and business challenges are addressed in a coordinated manner, what is more likely to emerge is a fragmented and incompatible tangle of proprietary solutions and regional alliances with no easy path to convergence.

Although many issues are still unresolved, the industry should at least rally behind the following strategically important points:

- Standards-based solutions should be used whenever practical.
- Authentication should migrate to 802.1X and WPA, which have superior security properties and permit greater flexibility in credential types than browser hijack. However, both browser hijack and 802.1X will coexist for at least a few years.
- Accounting data suitable for all billing models should be collected.
- Roaming intermediaries such as aggregators and clearing houses will help solve scalability issues and provide interoperability with legacy authentication and billing systems.

The hotspot blueprint architecture derived from this study will be implemented and tested in a validation test bed by a variety of carriers and vendors in the Asia Pacific region. Results from the test bed, including feedback from participating carriers, vendors, and other interested parties, will be used to develop specific deployment recommendations for WLAN client vendors, hotspot operators, and AAA providers.

## ACKNOWLEDGMENTS

The authors thank Jesse Walker, Lakshmi Ramachandran, and Sameer Pareek for their contributions to this paper.

## GLOSSARY OF ACRONYMS

This glossary will help the reader navigate the many acronyms used in this paper.

| Acronym | Definition |
|---|---|
| AAA | Authentication, Authorization, and Accounting |
| AAA-H | Home provider AAA server |
| AAA-V | Visited network AAA server/proxy |
| AP | access point |
| ATM | Asynchronous Transfer Mode |
| AES | Advanced Encryption Standard |
| CIBER | Cellular Intercarrier Billing and Exchange Roaming Record |
| DCH | Data Clearing House |
| DNS | Domain Name Service |
| EAP | Extensible Authentication Protocol |
| GSM | Global System for Mobile Telecommunications |
| ISP | Internet Service Provider |
| IEEE | Institute of Electrical and Electronic Engineers |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| INT | Roaming intermediary |
| IPDR | Internet Protocol Detail Record |
| LAN | Local Area Network |
| PEAP | Protected EAP |
| RADIUS | Remote Access Dial-In User Service |
| SIM | Subscriber Identity Module |
| SSID | Service Set Identifier, a unique 32-bit identifier for WLANs |
| TAP | Transferred Account Procedure |
| TKIP | Temporal Key Integrity Protocol |
| TLS | Transport Layer Security |
| TTLS | Tunneled TLS |
| UAM | Universal Access Method |
| USIM | Universal Subscriber Identity Module |
| VLAN | Virtual LAN |
| VPN | Virtual Private Network |
| WEP | Wired Equivalency Privacy |
| WISP | Wireless ISP |
| WLAN | Wireless Local Area Network |
| WPA | Wi-Fi Protected Access |
| WS | Wireless Station |

## REFERENCES


- [1] "Enterprises Must Consider Six Types of WLAN 'Hot Spots'," Gartner, June 2003.
- [2] Transport Layer Security, published as IETF RFCs 2716 and 3546.
- [3] Wi-Fi Protected Access, http://www.wi-fi.org/OpenSection/protected_access.asp
- [4] The IEEE 802.1X standard, http://standards.ieee.org/getieee802/download/802.1X-2001.pdf
- [5] Extensible Authentication Protocol, IETF RFC 2284bis (ongoing).
- [6] Protected EAP, IETF draft-josefsson-pppext-eap-tls-eap-06.txt (ongoing).
- [7] Tunneled TLS, IETF draft-ietf-pppext-eap-ttls-02.txt.


## AUTHORS' BIOGRAPHIES


**Prakash Iyer** is a senior staff architect in Intel's Network Architecture Lab. In his 11+ years at Intel, his areas of focus have included 10/100 Mbps Ethernet, IP Telephony and video conferencing, IPv6, networking security, and residential networking. He currently leads a research team focused on advanced wireless technologies. Prakash was the chair of the UPnP Internet Gateway group in the UPnP Forum and was a 2002 recipient of the Intel Achievement Award for his UPnP work. He holds B.S. degrees in Physics and Electrical and Computer Engineering and an M.S. degree in Computer Science. His e-mail is prakash.iyer@intel.com

**Victor Lortz** is a software architect in Intel's Network Architecture Lab. In his nine years at Intel, his areas of focus have been object-oriented software development, home networking, network security, and wireless mobile networking. Victor is the chair of the UPnP Security Working Committee. He was a 2002 recipient of the Intel Achievement Award for his UPnP work. He holds a B.A. degree in Physics from Whitman College and M.S. and Ph.D. degrees in Computer Science from the University of Michigan. His e-mail is victor.lortz@intel.com

**Lee Tapper** is a program manager and business development manager in Intel's Emerging Platform Lab. Lee works on 802.11 programs and was a member of the GSMA's WLAN task force. Lee holds a BSEE degree from the University of Texas. His e-mail is lee.s.tapper@intel.com

**Roger Chandler** is a market development manager in Intel's Emerging Platform Lab. His areas of focus have included manufacturing process analysis, high-performance 3D technologies, and home networking. He was a 2001 recipient of an Intel Achievement Award for his work in the field of Web 3D. He is currently focused on market development strategies for Intel's many wireless technology initiatives. He holds an MBA degree from the University of Georgia and a B.A. degree from the University of Tennessee. His e-mail is roger.d.chandler@intel.com

**Roxanne Gryder** is a business development manager in the Networking Architecture Lab, Intel R&D. She is involved in business and marketing activities for a variety of wireless technologies in the labs. She received B.S. and MBA degrees from Northwestern University and Cornell University, respectively. Her e-mail is Roxanne.r.gryder@intel.com

Copyright © Intel Corporation 2003. This publication was downloaded from http://developer.intel.com/.

Legal notices at http://www.intel.com/sites/corporate/tradmarx.htm.

For further information visit:

developer.intel.com/technology/itj/index.htm

Copyright © 2003, Intel Corporation. All rights reserved.
Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.
For a complete listing of trademark information visit: www.intel.com/sites/corporate/tradmarx.htm