Key RADIUS/AAA Considerations for Hotspot Operators

December 2005

A Juniper Networks company

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
(617) 497-6339
http://www.funk.com

Executive Summary: Choosing a RADIUS server to support your current and future hotspot business models

WLAN access at hotspots is still a relatively new phenomenon, and not surprisingly there is no consensus which hotspot business model — or which mix of models — will prove most profitable for hotspot operators.

Most hotspots today operate on the *open access model*, in which users can sign up via their Web browsers, and pay on-demand or be billed against an existing provider account. But while open access is secure enough for recreational Web access — and simple enough to attract "walk-in" business — it is by no means a final solution. Because it doesn't protect user credentials and data transfer over the wireless connection, open access is not secure enough for most corporate users, or for individuals concerned about identity theft and other personal security issues. And open access doesn't offer you the management and delivery control you need to offer customized services that can increase customer loyalty, reduce churn, and generate incremental revenue from customers.

For these reasons, eventually you'll implement at least one additional hotspot business model that lets you offer more secure, premium wireless Internet access to hotspot customers who want it — and most likely you'll base that model on the *802.1X* security standard, used by most corporations to secure their WLAN access. If you also offer GSM wireless phone service, you may want to implement *SIM-based* or *SMS-based authentication* that lets you offer wireless hotspot Internet access to your existing wireless phone customers, based on the information in your subscriber database (and conveniently bill customers for both on a single statement).

Whichever model you use now or plan to use later, you need a RADIUS/AAA server to authenticate users and account for their usage. Consequently it makes sense to choose a RADIUS/AAA server that supports authentication in open, 802.1X, and, possibly, SS7 or SMS environments. If this server comes from a manufacturer with a track record of supporting new WLAN authentication methods as they emerge, so much the better.

This white paper covers

- The workings, practical advantages, and security risks of the open access model;
- The security advantages, business benefits, and infrastructure requirements for implementing 802.1X, 802.1X with SIM-based authentication, and SMS-based authentication;
- The requirements you should look for in a RADIUS/AAA server designed to support authentication and billing in these and other emerging hotspot business models.

This paper assumes a high-level understanding of RADIUS/AAA.

Open Access

Open access is the most prevalent type of hotspot access today. Here, an end user goes through a sign-up page prior to being granted access to the Internet. When the user signs up, his payment information is either processed directly against a credit card system, for "on-demand" access; or, if he has or is opening an account, his login credentials are verified against a RADIUS/AAA server. If his credentials are valid, and his account active, he is granted access to the public network.

From an operator's standpoint, open access presents the following advantages:

- **It's relatively easy to set up**. Setting up open access requires very little beyond the supporting infrastructure you already have. You simply need to add access points and an access controller.
- **No client or other type of software is required on the user's wireless device**. The client device does need to be running Wi-Fi hardware – but this is typically inexpensive or built in to new laptops. In essence, anyone with a browser and a wireless card is a potential customer.

For these reasons, open access quickly became the norm in hotspots, and continues to be an ideal technology for attracting and keeping the casual "walk-ins" who currently make up the majority of hotspot WLAN users.

However, despite these advantages, open access does not provide any security. Specifically, users connecting in open access hotspots face the following dangers:

- **No data security**. Session data passes unencrypted between the users' computer and the access point; anyone within range can read email, and view all other personal data as it travels across the wireless link.
- **No mutual authentication** — that is, users can easily be tricked into connecting to an illegal network. All an intruder needs to do is set up a rogue access point, induce hotspot users to connect to it, and capture all the data they transmit.

Of course, it's not news to anyone that open hotspot access isn't secure, and today the majority of hotspot users still have little or no expectation of privacy as they surf the web and sip their coffee. However, it is likely that this situation will change. As users hear and read more and more reports of stolen credit card information, compromised privacy and stolen data, a growing number will want hotspots that can provide more secure wireless connectivity.

The most likely technology that secure hotspot access will be based on is the IEEE security standard 802.1X.

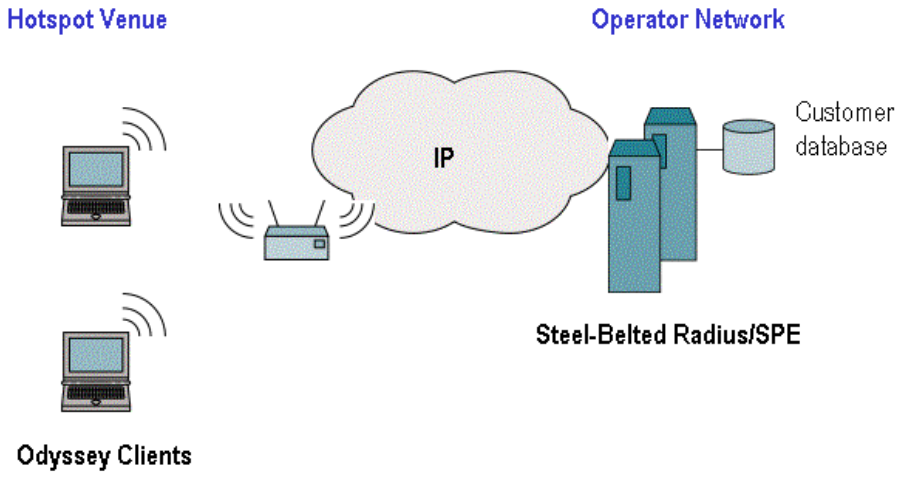
802.1X

802.1X protects against the security dangers present in an open access model. Offering secure hotspot access via 802.1X offers many advantages to operators, the main one being it allows you to generate incremental revenue by selling new services – that is, secure hotspot access – to new and existing customers. With 802.1X you'll be able to reach:

- **Casual users interested in protecting their personal data** – users who want to send email, view their calendars, and more without having to worry about their credit card information or other data being compromised.
- **Corporate accounts.** On a higher level, your secure offerings will likely appeal to security officers at large corporations who would like to wholesale secure access from a trusted provider. Even if corporate users customarily open VPN connections back to their offices, 802.1X provides additional security that the VPN doesn't. In particular, 802.1X provides for mutual authentication of the client and network, so users know they're connecting to a trusted network; and encrypted credential exchange, to protect against identity theft. In addition, 802.1X offers the additional benefit of providing the same user experience whether a user is connecting at work or at a hotspot, which will simplify their support load and user training requirements.

With these new business opportunities, it likely makes sense for your business to evaluate offering 802.1X-based access.

802.1X-based hotspot access



How 802.1X secures hotspot access

802.1X provides complete security against the known hazards of wireless computing. In 802.1X a hotspot user is not allowed access to the public network until he has been successfully authenticated against a customer database;

authentication can be based on user name and password, certificate, or SIM-based credentials.

An 802.1X-compatible RADIUS/AAA server checks the user's credentials against the customer database. If the user is authorized, the RADIUS/AAA server distributes encryption keys to the access point, and these keys are used to secure the wireless link.

802.1X, in conjunction with a secure Extensible Authentication Protocol (EAP) type (see the sidebar) provides the following security for the hotspot user:

- **Credential exchange is protected over the wireless link**. In 802.1X a user's credentials are never subject to dictionary attack or other intrusion techniques.
- **Mutual authentication of client and network**. The authentication process ensures both that the client is authorized to connect – that is, his credentials are verified against the customer database – and that the client is connecting to a trusted network. Note that the client does not present user credentials until it trusts the network.
- **Ensured data security via dynamic WEP, WPA, or 802.11i (WPA2) encryption.** The use of WPA or WPA2 is recommended, as it provides significantly stronger data security over the wireless link.

(For more information on 802.1X, see Funk Software's white paper "Secure Authentication, Access Control, and Data Privacy on Wireless LANs".)

EAP Types

EAP (extensible authentication protocol) types differ in both the level of security they provide and the ease with which they can be implemented and managed. The most commonly-deployed EAP types today include:

EAP-TTLS is an IETF draft jointly authored by Funk Software and Certicom, and is a working document of the PPP Extensions group. EAP-TTLS provides secure user authentication, using a TLS tunnel to encrypt password-based credentials that would be otherwise subject to dictionary attack on the wireless link. It provides strong security, while supporting legacy password protocols, enabling rapid deployment against your existing security infrastructure.

EAP-PEAP is similar to EAP-TTLS, and provides a similar level of security. However, with EAP-PEAP, only EAP may be carried as a protocol inside the tunnel. For this reason, EAP-PEAP is appropriate for use against Windows Active Directory and domains (via EAP-MS-CHAP-V2).

EAP-SIM is the SIM protocol used for authentication on SS7 networks carried within EAP, making it available for use on IP networks.

EAP-TLS is a follow-on to Secure Socket Layer (SSL). It provides strong security, but relies on client certificates for user authentication. It is mostly used in organizations which have already deployed a PKI infrastructure.

EAP-LEAP is the Cisco protocol that was widely used in the enterprise market, but is now being retired by most users in favor of one of the protocols above.

Infrastructure Considerations

802.1X access requires 802.1X-compatible equipment and RADIUS/AAA servers. In addition, each hotspot user must run an 802.1X-compatible wireless card, and client software (also called a "supplicant"). You can choose to:

- **License an 802.1X client and distribute it yourself**. While this option requires engineering work on your part, it also presents attractive branding opportunities.
- **Publish a list of preferred 802.1X clients**. This option provides your customers with a roadmap to source the client, and also simplifies your support requirements.

You will also need to decide which secure EAP method(s) you'll require (again, see the sidebar). This choice is largely determined by your authentication scheme:

- If you authenticate user name and password credentials, you'll require EAP-TTLS or EAP-PEAP.
- If you authenticate SIM credentials, you'll require EAP-SIM. Note that this requirement is the exclusive domain of GSM operators; for more information, see the next section "802.1X with SIM-based Authentication".
- If you authenticate certificate credentials, you'll need to use EAP-TLS

802.1X with SIM-based authentication

If you're a GSM operator, you too can offer your subscribers all the benefits of 802.1X-based hotspot access. However, to do so you face a somewhat more advanced set of requirements:

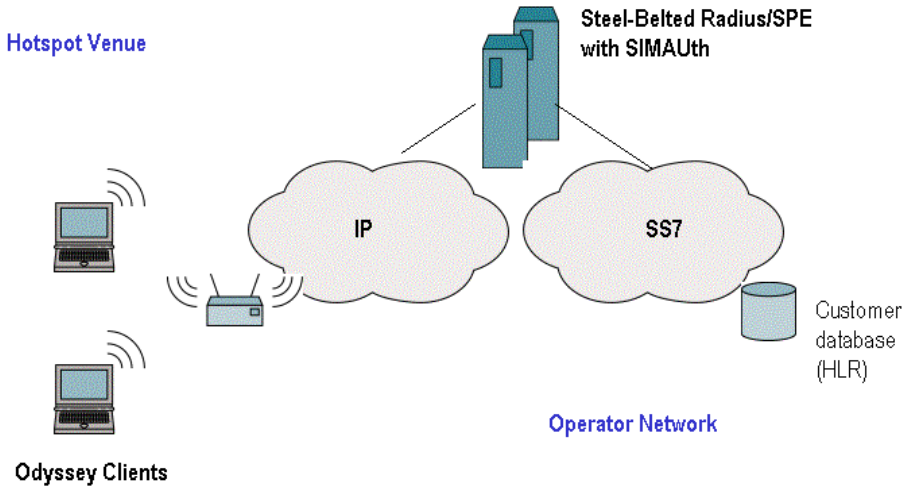
- You may want to deliver services and bill according to information stored in your existing subscriber database (HLR) – which is of a different format than that used on the public WLAN, and is based on SS7 technology
- Authentication and service delivery based on information stored in an HLR is not usually a feature of RADIUS/AAA servers; you will need to add this functionality to your RADIUS/AAA server, in addition to ensuring its 802.1X compliance

These challenges are addressed by implementing an infrastructure with the following components:

- **An SS7 interface** which provides the gateway between the public WLAN and your SIM-based infrastructure. SMS gateways typically comprise signaling software and a T1/E1 interface card.
- **A RADIUS/AAA server that supports EAP-SIM**. EAP-SIM permits the use of SIM in an 802.1X environment.
- **802.1X-compliant access equipment and RADIUS/AAA server.**

In addition, an 802.1X client is required on each wireless device.

802.1X-based hotspot access with SIM-based authentication



With this infrastructure, you can authenticate SIM-based credentials against your subscriber database, and deliver secure hotspot access to your subscribers. You can also capitalize on your existing roaming infrastructure: Once you put business terms in place with your roaming partners, you will be able to offer your customers access from a wide variety of hotspots, whether they are under your control or not. (As you are likely aware, the GSMA organization is currently working to standardize the process associated with roaming between public WLAN providers.)

SMS-Based Authentication

If you are a GSM operator and choose not to implement 802.1X – or if your timeline for adoption is farther out – you can implement a hybrid approach that relies on out-of-band delivery of login credentials (via the SMS text messaging protocol).

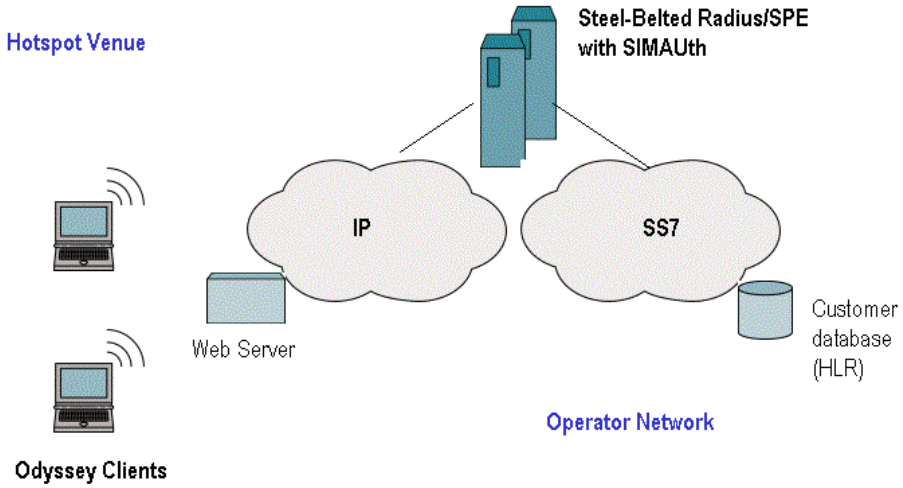
In this model, which does not require 802.1X, a subscriber is authenticated against the HLR, using an SS7 gateway solution; once authenticated, the HLR delivers to the end user's mobile phone, via an SMS message, the user name and password with which to log in to the network.

This method offers the following advantages:

- **It lets you offer WLAN access based on information in your subscriber database (HLR).**
- **It uses a common delivery mechanism you may already be employing in support of other services** — that of delivering confirming information to users' mobile phones.
- **It minimizes the possibility of fraud.** Because login information is delivered to a user's phone, it's more likely that the owner of the account is the one accessing the network.

- **It doesn't require upgrading your infrastructure to 802.1X**, or require client software on the wireless device.

Hotspot access based on SMS-based authentication



Beyond the anti-fraud protection offered by delivering login credentials to the mobile phone, no other security is provided in this model.

RADIUS/AAA Requirements

To ensure that you'll be able to implement open access, 802.1X, or any other hotspot access model — and to get the most from your investment in whatever model(s) you implement — you need to choose a RADIUS/AAA server that:

- **Provides complete and flexible compatibility with your back-end systems**, so that you can authenticate seamlessly against your existing user database or directory and automatically transfer usage data to the accounting and billing systems you have in place.
- **Supports the widest range of EAP types.** Since you may have no control over which 802.1X clients and EAP types corporations or users will choose, it makes sense to choose a AAA server that supports the widest range of EAP types, so that you can support as many clients — and consequently, as many users — as possible. At the very least your AAA server should support the more-secure PEAP, EAP-TLS, EAP-TTLS and EAP-SIM/AKA. Also, because wireless software and equipment vendors continue to develop new EAP types, make sure your AAA vendor has a history of supporting new EAP types as they emerge.
- **Works with virtually every brand of 802.1X equipment, including dual-mode equipment.** Avoid proprietary AAA servers that lock you in to a single brand of equipment. Choose a server that supports any 802.1X equipment out there, so that you — and your hotspot proprietors — are free to choose the equipment that best meets your performance requirements and budget. Also, since you'll almost certainly want to continue offering open

access, make sure your AAA server works with *dual mode equipment* — equipment that supports both 802.1X and UAM/WiFi access.

- **Provides the reliability and performance you need.** Reliability is critical; in particular, dropped or lost RADIUS accounting messages will cause problems reconciling bills from hotspot operators, and could lead to lost revenue. Insist on a AAA server with carrier-class reliability and capacity to handle peak traffic from hotpots, and reliable delivery and reconciliation of accounting data, which forms the bases of settlements with your customers and roaming partners.
- **Offers SS7 and SMS gateway functionality** to support authentication via GSM mobile phones.

When implementing 802.1X access, be sure to choose a client that supports multiple EAP types, is easy to use, is easy to deploy, and can be updated or configured centrally (i.e., without requiring a desktop visit).

Funk Software's Flexible RADIUS/AAA Solutions for Hotspot Access

Open access, 802.1X, and SIM/SMS-based authentication each offer different practical advantages and revenue opportunities for your hotspot Internet access business. To equip your infrastructure to take maximum advantage of these opportunities, you need a RADIUS/AAA that supports them all — and that works with whatever infrastructure hardware and back-end data systems you have in place today, or might adopt in the future.

Funk Software's award-winning Steel-Belted Radius server meets the authentication, authorization and accounting requirements of any open access, 801.1X or SMS-based authentication model — or any combination of these models — that you plan to implement today or in the future. It supports WLAN hardware from virtually every leading vendor, including emerging dual-mode hardware designed to support both open and 802.1X access. It authenticates seamlessly against any user database and writes to any back-end system you use for accounting and billing. It supports every leading EAP type, including the very-secure EAP-TTLS and EAP-PEAP. Used by some of the world's largest Internet and telecommunications service providers, it delivers the performance, reliability and robust accounting required to support carrier-class usage levels and the most complex roaming arrangements. And it provides optional SS7 and SMS gateways to support authentication via GSM mobile devices.

Funk Software's Odyssey Client is a universal 802.1X client that runs on Windows XP/2000/98/Me and supports every leading EAP type. Odyssey client can be centrally deployed and configured, and customized to reinforce your brand.

For more information on how Steel-Belted Radius and Odyssey can help you get the most from your current and future hotspot infrastructure investments, contact Funk Software at 1-617-497-6339, or at sales@funk.com.

A Juniper Networks company

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
(617) 497-6339
(800) 828-4146 (US/Canada)
http://www.funk.com