Jacques Caron

INTERNET-DRAFT
Expires: August 2002

IP Sector Technologies

February 2002

Public Wireless LAN roaming issues

<draft-caron-public-wlan-roaming-issues-00.txt>

1 Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

2 Abstract

Public wireless Internet access zones based on IEEE 802.11 [1] wireless LAN technology are becoming common. However, many issues are impeding further adoption of the technology by end-users, in particular the inability or difficulty to roam between the networks of different providers. This document aims to document these issues, show how they are different from roaming in other contexts such as dialup access to the Internet or GSM roaming, and how current solutions do not fully address these issues. Future documents will try to address these issues with practical solutions.

Table of Contents

3 Introduction

Public wireless Internet access zones (also known as "hot spots"), commonly based on IEEE 802.11 wireless LAN technology are becoming common. However, many issues are impeding further adoption of the technology by end-users, in particular the inability or difficulty to roam between the networks of different providers.

The rest of this document is structured as follows. Section 6 gives a brief description of the workings of public wireless Internet access zones. Section 7 shows why roaming is so important in this context, and how it is different from other roaming environments, such as dialup Internet access or GSM roaming. Section 8 describes current solutions used to address authentication and possibly roaming. Section 9 describes the issues found in these setups and other possible issues.

4 Terminology

WISP Wireless Internet Service Provider. An organization which provides access to the Internet via Wireless LAN infrastructure.

WLAN Wireless LAN, using e.g. IEEE 802.11 protocols.

5 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

6 Public Wireless Internet access zones

Public wireless Internet access zones are locations equipped by Wireless Internet Service Providers (WISPs) with appropriate hardware so that any user with a device (such as a laptop or PDA) and an appropriate network card can attach to the wireless network, access the Internet, and use any application relying on it, such as e-mail, WWW browsing, remote access to a corporate network (VPN), etc. while present in the coverage area.

Currently, most such setups rely on the IEEE 802.11 Wireless LAN technology, which provides cheap and fast connections (up to several megabits per second), and a reasonable coverage area. The technology is also extensively used within corporate and home boundaries, which allow the reuse of existing hardware and minimum reconfiguration.

Such an access zone usually consists of one or more access points providing the interface between the wireless devices and the wired network, and some form of access controller (which may be integrated within an access point) which checks that the user is properly authenticated and authorized, and may perform such functions as accounting, online subscription, provide local information services, etc. The whole setup is then connected to the public Internet.

In most cases, authentication and authorization is actually relayed to some central server holding the database of authorized users. When roaming between different providers is implemented, additional relaying can occur until the appropriate server is reached.

7 Roaming requirements

For the public WLAN access model to become widely accepted, it is necessary to build up critical mass, by having very extensive coverage, without the need for users to sign up with multiple different providers.

This requires roaming, as can be found in Internet dialup access (discussed at length in the works of the roamops working group [3,

4]) or GSM networks, but an important difference makes it even more of a requirement: the limited coverage of WLAN networks.

Internet dialup relies on the existing PSTN (public switched telephone network) infrastructure, which allows for access from nearly any location in the world (even though it might come at a

cost). It is not uncommon in many countries to have "nationwide" numbers which allow Internet access for the price of a local call from anywhere in the country. This means that a single ISP participating in the roaming system the user subscribes to is enough for that whole country.

GSM networks have cells that can cover up to hundreds of square kilometers, and often have regulatory requirements for widespread coverage. Hence, here also, a single GSM operator in the country having a roaming agreement with the home GSM network is often enough. In the worst case, the number of GSM operators in a country is anyway limited to a very small number, usually a handful at most.

In comparison, a WLAN cell coverage radius is only a few hundred meters. For this reason, WLAN coverage by any given operator remains limited, and a much larger number of operators of all sizes (from one access point to several thousand or more) will be required to get any decent coverage and reach critical mass.

7.1 Transparent roaming

Like for Internet dialup or GSM roaming, it is felt necessary that authentication of users roaming to a public WLAN should be transparent, i.e. does not require any manual action from the user, or the use of a specific application.

The first point is that no specific reconfiguration should be needed when roaming, not only from one public WLAN to another, but also from a private WLAN (at home or at work) to a public one, and vice versa.

It is also important to make sure the public WLAN can be used for any IP-based service, including e-mail, VoIP, corporate VPN access, etc. without requiring prior launch of a web browser, for instance, which might not even be implemented on the specific device being used (such as a VoIP phone).

7.2 Security

Due to the very nature of wireless technology, authentication exchanges must be protected against eavesdropping, which includes capture of clear-text passwords, but also offline dictionary attacks against encrypted credentials.

Given the wide number of WISPs of all sizes that will be used, it is difficult to ascertain a trust relationship with every one of them. For this reason, it is imperative that credentials be protected end-to-end, i.e. between the client and its home authentication server.

WLANs also allow the easy set up of "rogue" access points (a problematic which does not exist in the dialup or GSM world), that could attempt to act like a legitimate access point to try to capture credentials. This again requires end-to-end protection of login information, as well as means for the user to be sure that the access point has access to its home server (mutual authentication).

Due to the possible lack of trust, and the probability that billing will be at least in part duration based, it is also important that home authentication servers (and indirectly users) can be sure that visited networks cannot "cheat" on accounting by extending session durations beyond their real lifetime. For this reason, it must be possible for home servers to periodically re-authenticate roaming users.

Conversely, it is also important for WISPs to make sure they will be paid for the services provided, and hence have non-repudiation mechanisms in place. This is detailed in section 7.4.

Another problem is the ability for another user to eavesdrop on a legitimate user connection, take note of MAC and IP addresses, and take its place as soon as the previous user left. This should be addressed by some kind of local and/or end-to-end periodic re-authentication.

7.3 Scalability

Given the very high number of WISPs that will be needed to get decent coverage, and the need for global roaming, the roaming system must be highly scalable. It is also doubtful - and undesirable - that one single organization (roaming broker) will be able to build relationships will all actors in the market, and handle them efficiently.

It this thus necessary to envision an "open" roaming model, which would allow for more complex chains of roaming intermediaries between a network operator and a home authentication server, much like Internet routing can go through a complex path through multiple ISPs with various peering and transit relationships.

Exactly like in the Internet where global connectivity is a requirement, it is very important that this open model ensure that roaming can be global, and that there is always a path between any network operator and any authentication server.

7.4 Cost transport and accounting

Due to the requirements for a scalable and open roaming model, and given the diversity of the cost structures of various WLAN operators, it is desirable that any protocols used for carrying

authentication and authorization requests also carry cost information.

This information must be described in a format that accounts for all known billing scenarios (duration-based, volume-based, flat-fee, pre-pay, initial and subsequent increments...), and can be easily parsed and interpreted. The data may be modified along the way to reflect roaming agreements (commissions of roaming brokers).

This information should also take into account different currencies, and it is expected that roaming brokers will handle the conversion between different currencies.

This cost information should be present in:

- authentication/authorization requests sent to the home server (which might refuse "too expensive" connections based on the requesting user's plan, for instance);

- in requests presented to the client during the authentication process, so the user can approve (eventually in an automated fashion) the costs that are presented;

- in positive authorization responses, with a means to certify that the responding entity (home server or intermediate broker) agrees to these costs (e.g. a digital signature);

- in interim and final accounting messages;

- in accounting message confirmations, with a non-repudiation mechanisms such as a digital signature.

Note that the cost information and any digital signatures are only local to the relationship between any two operators (or between the end user and the home server, in the case of costs presented to the end user), since intermediaries are able to modify these costs.

Digital signatures or equivalent mechanisms might also be needed on the client acceptation of the costs presented.

7.5 Private access

Given the fact that contrary to dialup and GSM technologies, WLAN technologies are very often used in the home and office environments, it is important that any solutions used for public access be compatible with private access, without the need for complex reconfiguration.

It might also be possible to encourage operators of home and corporate WLAN networks to provide both private and public access, and handle appropriately different classes of users.

7.6 Other requirements

It is necessary that users that are not properly authenticated be able to get access to some resources, such as free local resources, servers providing service information and on-line subscription, help or customer service information, etc.

This might be achieved by assigned such customers to a distinct VLAN and/or IP network, or through filtering.

As much as possible, emphasis should be placed on solutions that can be easily used, ported, and installed on a wide variety of platforms, and not have too many dependencies on specific hardware, firmware, drivers or operating systems.

It is also important that any solutions allow easy roaming to and from other types of wireless (and maybe wired) networks, in particular GPRS, due to the complementing nature of GPRS and WLAN access technologies (wide coverage at low speed vs. limited coverage at high speeds).

7.7 Non-requirements

Once the client is properly authenticated and authorized, the question of the protection of the data flowing to/from the client is often raised, given the nature of wireless technology.

It is however felt by the author that any local encryption on the wireless media only provides a false sense of security, since data could be then easily captured by untrusted WISPs once it reaches the wired network.

For this reason, use of end-to-end protection mechanisms, such as IPsec (e.g. for VPN access to a corporate network) or SSL/TLS (for web browsing or e-mail transfer) is a better solution that needs to be encouraged.

8 Existing setups

Most existing setups in public WLAN access zones (other than those where access is free and no identification is required) use some form of Web-based authentication and connection hijacking, described below.

8.1 Attaching to the wireless LAN

Access points are usually configured in the most "open" way possible: there is no authentication and no encryption, thus any user with a compatible device can attach to the WLAN and reach any other devices connected to the network.

8.2 Getting an IP address and other parameters

All configuration is usually done via DHCP [5], which allows the user device to get a lease for an IP address, and other parameters such as default gateway, DNS servers, etc. Here again, there is no authentication, and any user can get this information.

8.3 Filtering and connection hijacking

Until the user is properly authenticated and authorized, most traffic is not authorized between WLAN users and the rest of the global Internet. However, any attempt to reach a WWW server using

the HTTP protocol [6] over a TCP connection to the well-known port for this protocol (port 80), is captured locally, and results in a "redirect" towards a pre-defined target, usually a WWW server providing an authentication interface, as defined below.

An exception is made so that any user can get access to "free" resources, which include the WWW-based authentication server, and eventually service information, online subscription and online help servers.

8.4 WWW-based authentication

Here, a Web based interface allows the user to enter authentication information, usually a username and a password. The web server providing this interface can be either a device local to the hot spot, or some remote server to which access is allowed even if the user is not yet properly authorized.

The WWW interface is usually secured using the HTTPS [7,8] protocol (SSL or TLS [9]) rather than regular HTTP. This allows for protection from eavesdropping on the wireless LAN.

Once the user has provided appropriate credentials and they have been verified, filters are changed so that the user gets full access to the Internet.

8.5 Back-end systems

Back-end handling of authentication and accounting is not standardized, but it is believed to be often based on RADIUS, with the possible addition of proprietary extensions.

8.6 Issues with existing setups

It is pretty clear that the existing setups do not meet all of the requirements set forth in section 7, in particular:

- roaming is not transparent, user interaction using a WWW browser is required;

- roaming is not secure, data can be captured by rogue APs.

Beyond that, there is no standard solution to carry authentication information from the authentication gateways to the home server that would meet all the requirements, in particular:

- open, scalable roaming

- transport of cost information

- non-repudiation

9 Alternate solutions

One alternate solution lies in the use of IEEE 802.1X [10], an implementation of EAP [11] as a network port access control technique, together with appropriate EAP methods such as EAP TLS [12] or EAP SRP [13], as the network-to-client authentication interface. This would indeed satisfy many requirements, with the following issues remaining:

- 802.1X requires low-level integration into firmware, drivers and/or operating systems, both in the infrastructure and in the clients, which might delay its widespread adoption.

- there is a need to present cost information to the user, and get his/her acceptance of this cost, possibly within EAP.

Until 802.1X is widely deployed, an equivalent, but easily portable authentication method is required. Extensions to support cost presentation and approval are also needed.

On the back-end side, RADIUS or Diameter, transporting EAP, might constitute a good basis for the requirements set forth, however a number of extensions are needed:

- cost information encoding and handling;

- the ability to route authentication information for any user to its home server, via a possibly complex chain of intermediaries;

- non-repudiation mechanisms;

- in the case of RADIUS, additional security to compensate for the known deficiencies of the protocol.

10 Security Considerations

Security in a wireless roaming environment is paramount, and is considered in section 7.2 above.

11 References

1 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std.

802.11-1999, 1999.

2 RFC 2119 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

3 RFC 2914 Aboba, B. et al., "Review of Roaming Implementations", RFC 2914, September 1997

4 RFC 2477 Aboba, B., G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999

5 RFC 2131 Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

6 RFC 2616 Fielding, R., J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Bernlers-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", June 1999.

7 RFC 2817, Khare, R., S. Lawrence, "Upgrading to TLS Within HTTP/1.1", May 2000

8 RFC 2818, Rescorla, E., "HTTP Over TLS", May 2000.

9 RFC 2246, Dierks, T., C. Allen, "The TLS Protocol Version 1.0", January 1999

10 IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

11 RFC 2284, Blunk, L., J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", March 1998.

12 RFC 2716, Aboba, B., D. Simon, "PPP EAP TLS Authentication Protocol", October 1999.

13 <draft-ietf-pppext-eap-srp-03.txt>, Carlson, J., B. Aboba, H. Haverinen, "EAP SRP-SHA1 Authentication Protocol", July 2001, work in progress.

12 Author's Addresses

Jacques Caron
IP Sector Technologies
Ecluse 36c
2000 Neuchatel
Switzerland
Phone: +41 79 699 8389
Email: jcaron@ipsector.com