Chapter 9

Security in WiFi Roaming

9.1 INTRODUCTION

The primary reason WLANs were developed was to allow untethered connections between a client and an 802.11 access point (AP), as a basis for further access to resources and services on the Internet. The next step in this process is wireless roaming, in which a client can move across multiple APs in one administrative domain and across multiple APs across differing administrative domains. Currently, the most prevalent model for wired roaming consists of a dial-up connection from a client (e.g., a laptop) through an ISP, to a home domain (e.g., corporate network). This model presumes the prior existence of a business relationship between the client (or its corporation) and one or more Internet service providers (ISPs).

The term *WiFi roaming* can be loosely defined as the set of services supporting the deployment and management of 802.11 WLAN access at public venues or public *hotspots*, where the customer of one service provider can obtain services (e.g., IP connectivity) from a different (visited) service provider. The term *service provider* (SP) here is intentionally left abstract since in today's Internet a number of entities can take the role of providing one or more services relating to WiFi roaming. It is important to note that WiFi roaming involves the crossing of both network-administrative boundaries and security-administrative boundaries. Therefore, on-campus WLAN access at different remote locations (e.g., offices, buildings) under the same administrative jurisdiction is not considered here as WiFi roaming.[1]

The business case for WiFi roaming is self-evident: consumers with laptops or handheld devices are willing to pay for IP connectivity through WiFi hotspots located throughout the world, provided that WiFi access is easy to use and secure.

[1] This chapter intentionally uses the term "WiFi roaming" specifically for 802.11 WLAN access at public venues, which is different from access to a LAN or WLAN through separate 802.11 APs connected to the same LAN or WLAN. The term is also used to distinguish it from aspects of fast handoff between two APs connected to the same LAN or WLAN.

This desire is already true today, as seen in the case of dial-up IP services. Many traditional ISPs see WiFi roaming as providing a new business opportunity, by extending their edge services to a new kind of access point, namely, the public hotspot, while retaining as much as possible their investment in their existing backend authentication, authorization, and accounting (AAA) infrastructure.

For some *mobile network operators* (MNO) and carriers, the case for WiFi roaming can even be considered imperative, as they are seeking to augment and extend existing mobile-related services to their customers at affordable prices. Mobile handsets that can make use of WiFi hotspots — with speeds of 11 to 50 Mbps — could generate new business opportunities by providing users with higher-quality content and a higher level of interactivity. The case for WiFi roaming is of particular interest to MNOs that have invested heavily in the recent acquisition of 3G licenses.

Given the increasing mobility of the workforce, providing *secure* WiFi roaming is an important challenge today. Corporations see remote access as a given fact of life and expect services from their ISPs supporting remote access. This is true in dial-up today, and it is something expected of WiFi roaming in the near future.

In this chapter we look at the growing area of WiFi roaming. First, we review briefly the existing dial-up services, which are provided by many "traditional" ISPs. The dial-up AAA model provides a background for understanding the view of many ISPs and WISPs in providing WiFi hotspot services. This chapter then looks into the WISPr architecture for WiFi roaming, which is a proposal from a group of vendors and ISPs within the WiFi Alliance (WFA).

9.2 ROAMING IN DIAL-UP IP SERVICES: BACKGROUND

In the last decade, the combination of advances in portable computing technology (e.g., stronger laptops, PDAs), the finalization of the IPsec RFCs in the late 1990s, and the proliferation of dial-up services together promoted user mobility and the corporate acceptance of the notion the "road warrior" (traveling worker) and telecommuters. Thus, the three aspects of user mobility technologies, namely end-user devices, secure end-to-end communications, and IP-supporting services, combined to form much of what we understand — and take for granted — of the "mobile" Internet today.

From the perspective of IP communications mobility, the two most important developments in the last decade have been the establishment of dial-up services and the development of security protocols that protect IP communications end-to-end. These two areas of technology are important in the context of WiFi roaming because many of the concepts underlying WiFi roaming have been derived from the dial-up world. Indeed, existing ISPs and carriers want to retain as much as possible the dial-up infrastructures in the WiFi world in order to maintain their decade-long investments in these infrastructures. The public hotspot phenomenon has so far affected only the “edges” of the Internet. The core of the Internet has largely remained unaffected directly by WiFi-related technologies. Finally, the maturity of the IPsec (ESP) [1] and IKE [2] protocols has allowed IPsec-VPNs to be used over dial-up connections for remote access users. The same protocols continue to be used today over IP connections established at WiFi hotspots.

9.2.1 The Dial-Up Access Model

In the traditional dial-up access, a user uses a modem device to establish a connection to a *network services provider* (NSP), over the *public switched telephone network* (PSTN). The NSP, which is typically also an ISP, hosts a termination device for the PSTN connection (e.g., dial-up concentrators), which usually has IP switch/routing functionality. This is shown in Figure 9.1.

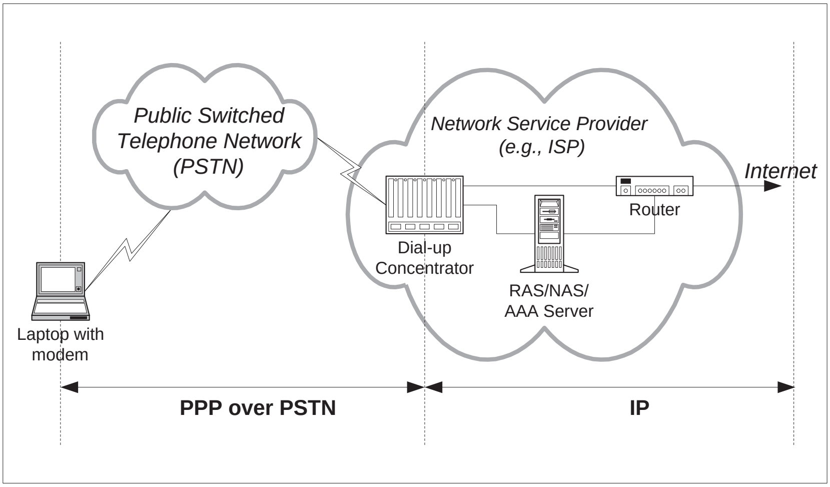

Figure 9.1 The traditional dial-up model.

In terms of IP connectivity, the connection between the user’s laptop/modem and the NSP is IP over the *Point-to-Point Protocol* (PPP) [3], which runs over the PSTN network. From the NSP onwards, the connection is IP over whichever medium the NSP uses with the ISP upstream (e.g., T1, leased lines, and so forth). The point here is that the PPP protocol is crucial for the dial-up connection from the user to the NSP.

Note that many dial-up NSPs provide a list of local telephone numbers and toll-free numbers to which the user can dial according to the user’s current location.

This approach is common today since most — if not all — PSTN networks in North America provide unlimited calls when they are made within the same area code. For traveling users, often a toll-free number is provided so that users need not pay for either local or long-distance calls.

From the security perspective, the dial-up connection over the PSTN provides better — though not much better — physical security compared to the broadcast nature of 802.11. In either case, an IPsec-VPN or SSL-VPN needs to be deployed to provide true end-to-end communications security.

9.2.2 Authentication in Dial-Up IP Services

In order to support authentication and authorization in dial-up connections, the PPP-Extensions Working Group in the IETF developed the *extensible authentication protocol* (EAP) in RFC2284 [4], with the most recent version of the protocol defined in RFC3748 [5]. For user authentication, typically a password-based protocol is used (e.g., CHAP [6] or MS-CHAP [7]), though EAP itself supports other protocols (e.g., EAP-TLS [8]) which use other forms of credentials (e.g., digital certificates).

When a user seeks IP connectivity over dial-up using PPP, as part of the set up a *PPP authentication* phase must be completed. Typically, the user dials against a *network access server* (NAS), which may or may not be collocated with the dial-up concentrator device (see Figure 9.1). The authentication of the user is done using EAP together with a specific authentication method chosen by the ISP.

Most ISPs prefer to use passwords as the basis for user authentication. Specific protocols implementing the challenge-response authentication model based on a (hashed) password include CHAP [6] and MS-CHAP [7]. This choice is driven by the fact that most ISPs use a simple database (e.g., LDAP) containing a table correlating user IDs, passwords, accounts, e-mail addresses, and other user/employer information.

9.2.3 The Network Access Identifier (NAI)

In the dial-up world, the identity of the user is known at the *network access identifier* (NAI) [9]. The NAI is the user identifier submitted by the client during the PPP authentication phase. Thus, the typical information submitted to an ISP from the client consists of the NAI and password pair. Depending on the specific password-based authentication protocol used, it is usually the hash of the password that is transmitted from the client to the ISP (i.e., NAS device at the ISP). This is to prevent snooping of the plaintext password when it is in transit to the ISP.

The NAI format is similar to the e-mail address, namely `user@realm` where the `realm` portion has the usual organizational domain ending. Although the NAI need not be an e-mail address, often ISPs prefer to use either actual e-mail addresses or some other information identifying the user's affiliation. Thus, for example, an NAI could be the e-mail address `johndoe@employer.com` where `employer` is the company employing the user and is the entity that established a business agreement with the ISP. Also, often a similar substitute may be used for the organizational name. For example, instead of using the `employer` realm, the ISP could use any other similar realm, such as `employerdial` or `employernetaccess` for example, where it is clear that the NAI refers to the same organization or company called "employer."

Although less secure, often ISPs assign an organization-shared password that is shared for all users of that organization. Rather than storing and managing a unique password per-employee or per-user, an ISP would simply assign a password to the entire organization, providing it only to the authorized IT administrators of that organization. It is then up to the IT administrator of the organization to set up the password and NAI correctly on the employee's dial-up application software. This approach is more practical, particularly from an identity-management perspective, bearing in mind that many dial-up ISPs employ the rudimentary LDAP database with RADIUS [10].

9.2.4 The NAI for Dial-Up Remote Access

In dial-up remote access, which has similarities to WiFi roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request. Typically, ISPs provide their customers with a list of numbers to dial in each country in the world where that ISP has a "presence," namely, a relationship with either a local PSTN or ISP (or both). This list is usually incorporated into the software dialer on the user's computer. The visited ISP needs the NAI to identify if the user is a customer of one of its business partners (another ISP) and it needs the realm information of the NAI in order to route an authorization request to that partner.

To illustrate the importance of the NAI, Figure 9.2 shows a simplified fictitious example of two users from the United States who are in France and dialing French ISP numbers.

Without going into details, `user1` is an employee of `Corporate1` whose provider happens also to be a mediator/broker. The second user, `user2`, is an employee of `Company2`, which obtains Internet services from a regular ISP. Both users are visiting Paris, France, and are dialing a telephone number that is served by the local PSTN, namely, France Telecom. In this example, `Corporate1` uses GRIC as their service provider in the United States, while `Company2` uses UUnet as their ISP in the United States. Coincidentally, both GRIC and UUnet have peering agreements with the same French ISP. Thus, although each user may dial a different number in Paris, their PPP connection is served by the same French ISP.

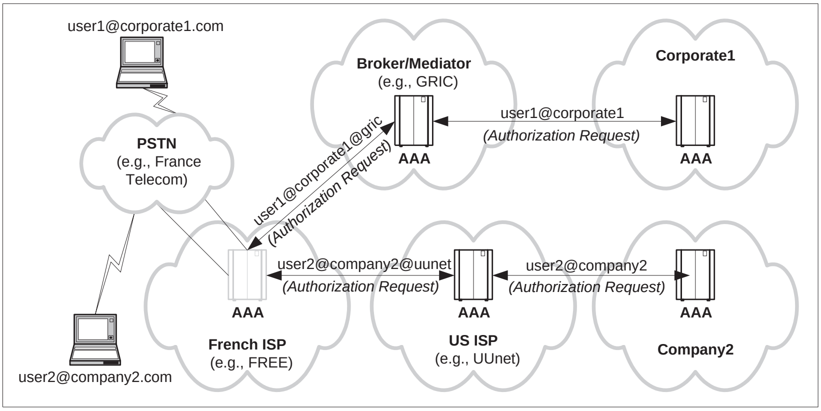

Figure 9.2 Example of NAI use in dial-up roaming.

In the case of `user1`, whose NAI is of the form `user1@corporate1.com`, the French ISP uses the realm information to forward the authorization request to GRIC since `Corporate1` is listed as a customer of GRIC. For `user2` with NAI `user2@company.com`, the French ISP forwards the authorization request to UUnet since the French ISP has a direct bilateral agreement with UUnet.

Note that the above example represents a fictitious example based on fictitious relationships. The aim is to illustrate the use of NAI by service providers for routing AAA-related parameters.

Furthermore, note that in order for service providers to provide WiFi roaming while retaining their AAA infrastructure (as shown in Figure 9.2), the only entity that essentially needs to be replaced in Figure 9.2 is that of the PSTN (replaced with a WiFi hotspot). Thus, instead of dialing a telephone number, the user would obtain 802.11 access at the hotspot, who would forward the authorization requests the same way as in our previous example of Figure 9.2.

9.3 WIFI ROAMING: ENTITIES AND MODELS

Roaming is about relationships among service providers. In order to carry over the roaming model from the dial-up world to the WiFi world, it is useful to understand the entities involved in both types or roaming and the roaming models that may apply to the WiFi world.

9.3.1 WiFi Roaming Entities

In order to analyze the issues and requirements relating to WiFi roaming, it is useful to understand the entities involved in WiFi roaming today (see Figure 9.3):

- *Hotspot wireless Internet service provider (WISP)*: This is the entity that actually manages and operates the 802.11 equipment and other network functions at a hotspot and has the relationship with an upstream ISP that provides basic high-speed IP connectivity out of that hotspot.

  For simplicity, and to avoid confusion, we identify these entities as WISPs, though today many traditional (wired) ISPs are also venturing into providing WISP functions. Thus, many ISPs can also be called WISPs.

  The term "wireless ISP" originated from the earlier days of hotspot footprint expansion and deployment. A handful of (start-up) companies adopted this business model at the outset of the WiFi revolution. However, the revenues coming from this business model proved to be so slim that these businesses were not sustainable. As a consequence, only established traditional (wired) ISPs, carriers, and MNOs could afford the initial rollout costs to enlarge the WiFi footprint to the point of being cost-effective and only such large players have remained today. Thus, it is not surprising today to find that traditional ISPs are providing WiFi hotspot services as extensions of the core ISP business.

- *ISP, carrier, or MNOs*: The ISP, carrier, or MNO is the entity that typically has a direct relationship with either the individual subscriber or the corporate customer (having many roaming employees). From an authorization point of view, all WiFi roaming access must obtain authorization from (or through) this entity, either in real-time or through some predefined (preapproved) service agreement.

- *Broker or aggregator*: A broker or aggregator is an entity whose role is to mediate among as many service providers as possible. It makes its revenue out of providing as large a number as possible of connections among its customers (ISPs, carriers, MNOs). Note that in recent years, some aggregators have begun to also own corporate customers directly, as a way to enhance their business model.

- *Corporate network*: This entity reflects corporate customers. Many enterprises in the past have required that dial-up authorization be obtained from the corporate network (i.e., the corporate AAA server). Thus, the same authorization model is also being adopted for WiFi roaming by some service providers.

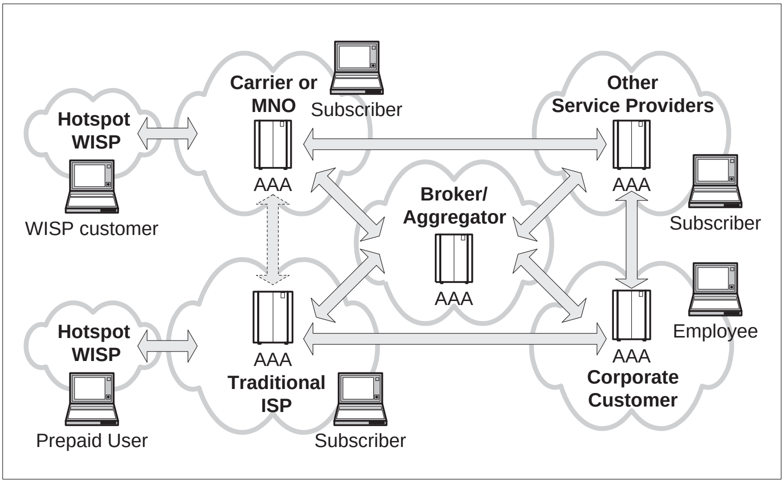

Figure 9.3 WiFi roaming entities and relationships.

It is important to note that although Figure 9.3 identifies three roles that provide services, in practice multiple roles (or all three roles) can be assumed by a single organization. Thus, for example, a traditional ISP could take on the first two roles by extending its services through additional hotspot footprints. Another example would be the case of the traditional carrier (Telco) who converts its public telephone booths into WiFi hotspots by adding an 802.11 access point and DSL modem atop (or instead of) its public telephone booths. Here, if the carrier is not an Internet ISP then the carrier would in fact be adopting the first role (hotspot provider) and the third role (WISP for billing and accounting). Finally, an entity could take up all three roles such as the case of an MNO who may already possess an ISP business unit and who now wishes to roll out WiFi hotspots with WiFi roaming capability for their customers.

9.3.2 Roaming Models

From a business perspective, three general roaming models are applicable to WiFi roaming. Which of these models are adopted in a given case is dependent on a number of factors, including existing business agreements, existing infrastructures and services, geographic locations, available software/hardware, and others.

In the following, we use the term *service provider* (SP) loosely, as it can refer to a new WISP, a traditional ISP, a carrier, MNO, or combinations of these. The three roaming models are as follows:

- *Bilateral model*. Here, a relationship between two SPs is assumed to exist where they enter into bilateral contractual agreement, allowing one SP's customer to use another's hotspots.

  In this model, each SP would need to maintain a list of originating domains, allowable users, and even some kind of routing table. In general, for a large number of SPs this model does not scale as each SP would need to enter into $n*(n-1)$ bilateral agreements with every other SP, where n equals the total number of roaming partners.

- *Roaming consortium model*. Here, a collection of SPs establish a roaming consortium that sets contractual roaming agreements for all its members. The consortium may also act as a clearinghouse that stores the routing table, list of member domains, and possibly a list of customers. Once set up, such a body can easily add new members who agree to participate in the pricing and billing structure established by the consortium organization.

- *Broker/aggregator model*. Here, an organization acts as a broker or intermediary between multiple SPs. In contrast to the consortium model, an SP may buy services from the broker on a more flexible and varied basis (e.g., on a per-use only basis). As such, this model may be more attractive to SPs compared to the consortium model.

  In this model, the broker maintains a relationship with each SP, negotiating pricing and other roaming support details independently and confidentially. An SP that signs up a relationship with the broker agrees to allow the broker to use other SPs, according to an acceptable *service level agreement* (SLA). Thus, for example, when a user roams into a visited hotspot, that hotspot provider (WISP) will forward the AAA session to the broker. If the broker is unable to authorize this session, it may forward it to the appropriate SP who can authorize it (e.g., the SP who actually owns the user).

The first two models represent the traditional model for (wired) ISPs, extended for WISPs. These models carry over much of the inherent operational difficulties of legacy authentication/authorization systems. Furthermore, they presume that business relationships exist among the concerned SPs, in order to manage and pass billing information among the roaming partners.

9.3.3 WiFi Roaming Security Requirements: A Classification

Aside from the security issues surrounding 802.11 technology, WiFi roaming has brought additional security issues that need to be addressed. In this section we briefly attempt to classify these issues according to a basic network topology that spans from the client (supplicant) to the corporate network. In looking at the criteria for classification, it is important to realize that in reality there are a number of ways the entities are involved and services are provisioned. Thus, a single solution to cover all these situations is impractical, if not impossible. Furthermore, the classification ignores the fact that business relationships exist between the entities and that the end-user can be a consumer (subscriber) that is "owned" by differing entities.

To simplify the discussion, we employ the notion of an *AAA session*, which can involve differing end points. For example, authentication could be against an ISP, while authorization is actually obtained from a corporate server (i.e., the user's employer) and accounting/billing is handled by yet another entity.

Figure 9.4 shows a simplified classification or grouping of security requirements in WiFi roaming, where again the term "service provider" (SP) is used to mean ISPs, WISPs, carriers, and MNOs. The basic idea here is that a client needs to be authenticated against a AAA server before the client can obtain IP connectivity at the WiFi hotspot. Typically, service providers only provide connectivity to the "open Internet" at the IP layer, beyond which the user/client needs to provide additional protection for traffic flowing over the IP connection (e.g., through IPsec-VPNs). The classification is as follows:

- *WLAN hotspot security requirements*. The segment of the AAA session between the client and first-hop AAA server or AAA proxy needs to be protected against various possible attacks, both at the IP layer and the 802.11 MAC packet layer. Both the IEEE and IETF communities today are working toward solving and standardizing solutions.

- *Inter-SP security requirements*. If an authentication session traverses SP boundaries, then protection needs to be provided for that session. This includes cases where a broker/aggregator is involved in the AAA session. This means that security mechanisms and policies governing provider-to-provider interaction needs to be deployed. Often, this interaction is dependent on the roaming model underlying the business relationship of the providers.

- *Intra-SP security requirements*. Several ISPs, carriers, and MNOs are large enough that they run dozens to hundreds of AAA servers and proxies within their own network. Thus, a AAA session must be protected even within the internal networks of SPs. Some SPs today use a permanent or semi-permanent IPsec-VPN or SSL-VPN between pairs of AAA servers in a fully connected graph fashion.

- *SP-to-corporate security requirements*. The last segment of the AAA session is often between a service provider with an enterprise, in the case of the roaming employee. In such cases, the final authorizer is the corporate AAA server. Note that in many instances, the authorization request (for the employee to obtain IP connectivity at a WiFi hotspot) need not go all the way to the corporate AAA server. Depending on the business agreement between the service provider and the corporation, the corporation may simply trust the service provider for all authorizations (e.g., up to a certain threshold or cost, based on some metric).

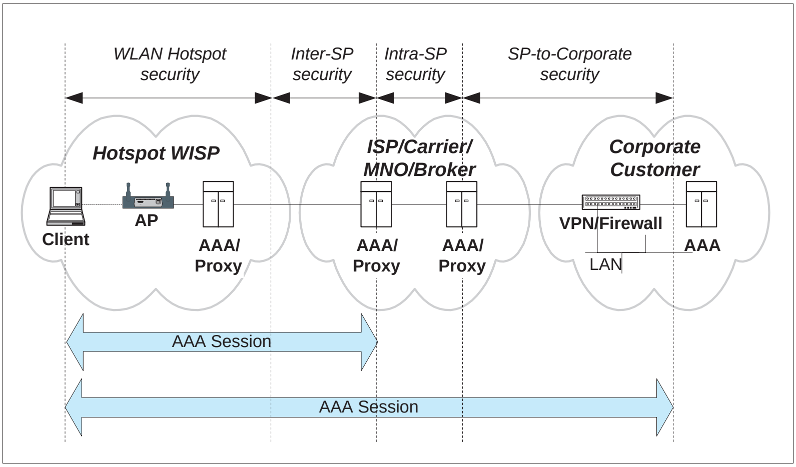

Figure 9.4 A classification of security requirements in WiFi roaming.

9.4 WISPR: THE WIRELESS ISP ROAMING ARCHITECTURE

As mentioned previously in Chapter 2, a small group of networking hardware vendors and ISPs inside the *Wireless Ethernet Compatibility Alliance* (WECA), called the *Wireless ISP roaming* (WISPr) group [11], began developing a framework for AAA function in the context of WiFi roaming. The WiFi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless LAN products based on IEEE 802.11 specifications. The WISPr group was chartered by WFA to describe the recommended operational practices, technical architecture, and authentication, authorization, and accounting (AAA) framework needed to enable subscriber roaming among WiFi-based WISPs [11].

In this section we briefly look at the WISPr example as an illustration of WiFi roaming in practice. The WISPr architecture is shown in Figure 2.2 in Chapter 2, while its topology is similar to that shown in Figure 9.4. A roaming user obtains WiFi services at a hotspot run by a hotspot operator (or WISP, in our current terminology). The hotspot operator runs the access points, one or more *public access control* (PAC) gateways, and one or more AAA servers (e.g., RADIUS [10] or Diameter [12]). A given AAA session may traverse through a "roaming intermediary" (which is optional), terminating at a *home entity*, which in practice could be the user's corporate AAA server or a AAA server at a home ISP. As mentioned in Chapter 2, for user authentication WISPr uses the Web-based password approach, called *universal access method* (UAM).

9.4.1 Hotspot Operational Aspects

The PAC gateway is used by hotspot operators to provide the access and services control in their WiFi network. The PAC gateway performs several key functions for the hotspot operator in order to support the UAM authentication method. Besides user authentication, the primary PAC gateway functions include the following [11]:

- *IP address management*. The hotspot operator or WISP needs to manage the user's IP address allocation, before authentication (over an IP connection) can occur. Note that this in contrast to the 802.1X authentication approach where IP address allocation is subject to a successful authentication.

  Several methods may be used for providing IP layer connectivity to the user. These include a DHCP lease to the user, or address translation for those users who already posses a static IP address. The PAC gateway may support DHCP server functions (and/or DHCP relay functions) to provide the user with a public or private IP address obtained from the pool of addresses belonging to the WISP. Note that if a private address is allocated, then in order to support a user's VPN, the PAC gateway has to perform address translation and support VPN protocols.

- *Home page redirection*. Crucial to the UAM approach is home page redirection, which provides the ability of the PAC gateway to intercept the initial HTTP request (destined to an *origin server*) of the user's browser. The user is then redirected to the WISP's welcome page. In order to prevent a man-in-the-middle attack on the user's username/password while in transit, an SSL layer must underlie the HTTP connection to the WISP's page. The PAC gateway needs to also include the ability to detect and adapt for browser proxy configuration, such as being configured to use a private proxy server. This assures that users are able to access the WISP's welcome page without having to reconfigure their browsers proxy settings.

- *Authorization*. The WISPr group has specified a number of *WISPr attributes* (for RADIUS) which must be supported by WISPs that participate in the WISPr initiative. Thus, during a given AAA session, a PAC gateway should enforce the services each user is authorized for as specified by the WISPr attributes (as returned by the home entity during the RADIUS authentication process). Examples of these attributes include service time periods and service bandwidth levels.

- *Accounting*. The PAC gateway must provide accurate and timely RADIUS accounting records for billing purposes. These accounting records must identify the location, duration, and service level of the call.
- *RADIUS client functionality*. In order to perform AAA functions, the PAC gateway must implement RADIUS-client functionality (as the PAC gateway will be a RADIUS client when interacting with the RADIUS server at the home entity). The PAC gateway must also provide for both explicit (active) and implicit (passive) logoff capabilities. In order to support explicit logoff, it should deliver a logoff pop-up to the user's browser. In either case, the event must trigger a RADIUS *accounting stop record,* containing information about the session duration and bytes transferred. The PAC gateway should also support RADIUS challenge-response using the RADIUS *access-challenge* messages.

9.4.2 AAA Sessions in WISPr

An example of an AAA session in the context of WISPr is shown in Figure 9.5. Here, the entities involved are similar to those mentioned in Section 9.3.1. The hotspot operator is the WISP, while the roaming intermediary in WISPr could be an ISP, carrier, MNO, or a broker/aggregator. The home entity can either be a corporation running (its own AAA server) or a "home ISP" with whom the corporate customer or the individual subscriber has a business relationship.

Figure 9.5 shows a number of events that reveal the importance of the PAC gateway in the WISPr architecture. In event 1 and event 2, the initial network connectivity (i.e., 802.11 association) between the client and the WISP occurs. Once the user opens his or her browser (event 3), an SSL session is opened between the client and the PAC gateway. The user's name/ID and password is then delivered protected by this SSL session (events 4, 5, and 6). The PAC gateway converts the user's name and password from the HTTPS connection to a RADIUS authentication message (event 7) and triggers the authentication process at the RADIUS server at the home entity. If the user is successfully authenticated by the RADIUS server and a RADIUS authentication-accept message has been received by the PAC gateway from the RADIUS server (event 8), the PAC gateway signals an accounting-start message to the RADIUS server (event 9). The accounting-start message indicates the beginning of the billable session and the user is automatically redirected to the start page of the WISP (as specified in the *vendor-specific attributes* list coming from the home entity in event 10).

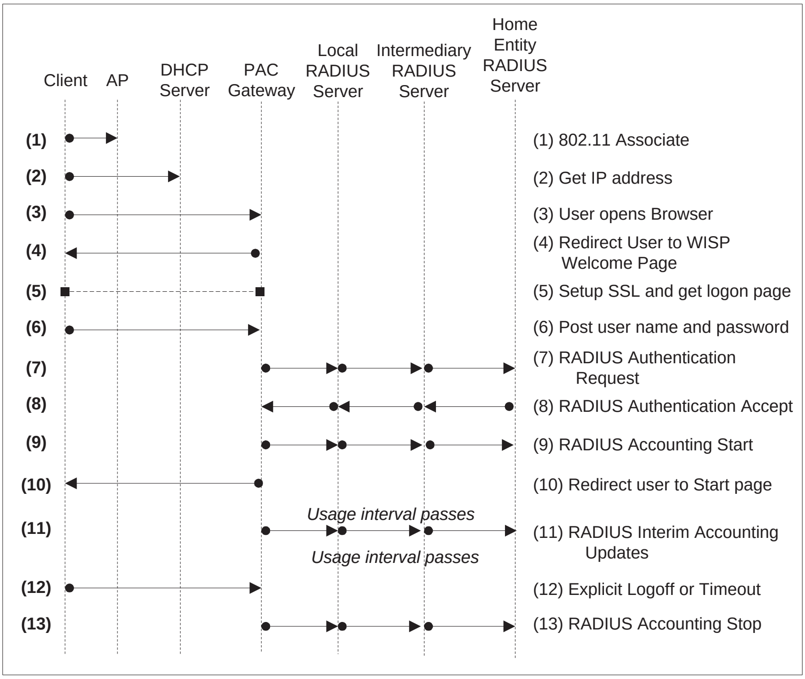
Client
AP
DHCP Server
PAC Gateway
Local RADIUS Server
Intermediary RADIUS Server
Home Entity RADIUS Server
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
Usage interval passes
Usage interval passes
(1) 802.11 Associate
(2) Get IP address
(3) User opens Browser
(4) Redirect User to WISP Welcome Page
(5) Setup SSL and get logon page
(6) Post user name and password
(7) RADIUS Authentication Request
(8) RADIUS Authentication Accept
(9) RADIUS Accounting Start
(10) Redirect user to Start page
(11) RADIUS Interim Accounting Updates
(12) Explicit Logoff or Timeout
(13) RADIUS Accounting Stop

Figure 9.5 Example of an AAA session in WISPr.

Throughout the connection session, periodic interim accounting updates are sent from the PAC gateway to the home entity (event 11). This is done periodically to limit the loss of accounting information should one or more of these entities crash or if some RADIUS messages are lost. The accounting update information is specified by the home entity in its RADIUS attributes list. Once the user is finished with the session and issues an explicit logoff (event 12), or if a timeout occurs, the PAC gateway sends a RADIUS accounting-stop message to the home entity, indicating the end of the user's connection session.

Note that the above basic events are not particularly new or unique to the WISPr approach and most of these steps are used today in dial-up RADIUS accounting. This reflects the conscious decision on the part of WISPr to provide a solution that interoperates with existing legacy authentication infrastructures that are found in many ISPs today, most of which are RADIUS-based.

9.4.3 Alternative Authentication Methods in WISPr

The deficiencies of the Web-based UAM approach for authentication has been described in Chapter 2. Among others, the UAM approach was not integrated into the key management function in the AP and the client and thus could not trigger the establishment of the appropriate keys for use by the encryption algorithm (i.e., TKIP) at the MAC packet layer.

Some members of the WISPr community, however, were aware of this problem and understood the longer-term need for better authentication. As such, the 802.1X authentication framework was proposed as an alternative to the UAM, with the authentication protocols suggested being PEAP and EAP-TLS. The PEAP approach was promising to many ISPs since it was compatible with the user-password approach with which many ISPs were familiar. In addition, since PEAP was an EAP method, the protocol was integrated into the key management aspects of 802.1X. Finally, from a deployment aspect in WISPr, PEAP was being supported by a major networking hardware vendor and thus provided the most promising avenue for a more secure WISPr solution going forward.

9.5 SUMMARY

The WISPr initiative presented one of the earliest efforts toward providing interoperability of WiFi roaming functions across WISPs, guided by a best practices document (BCP) that defined a standard Web-based user interface, a common network architecture, and a common set of RADIUS attributes for AAA requirements. Although WISPr itself was relevant toward providing a framework for all WISPs in the new field of WiFi roaming, the WISPr group itself was initiated within WECA (now WiFi Alliance), which is essentially a vendor compatibility and certification body. Hence, the primary interest of the vendors participating in WECA was to ensure that their products — hardware and software — correctly implemented the IEEE 802.11 and 802.1X specifications and were interoperable. Hence, although chartered within WECA, the WISPr group remained more or less a small unofficial group inside WECA.

Efforts to bring major carriers and MNOs to WISPr were unsuccessful at that time largely because these large companies were unsure about the future of 802.11 WiFi roaming (despite tremendous uptake of 802.11 gear by the home consumer market). They were also unclear about how to integrate WiFi roaming into their existing networks and unsure about the WiFi roaming business model. In addition, in North America many were in the process of migrating their networks to 2G and/or 2.5G technologies. Other similar efforts, such as *Pass-One* [13] in 2002, also met with difficulties in both the definition of their business model and in the uptake by vendors and operators in North America.

References

[1] S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP),” RFC 2406 (Proposed Standard), Internet Engineering Task Force, Nov. 1998.

[2] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409 (Proposed Standard), Internet Engineering Task Force, Nov. 1998.

[3] W. Simpson, “The Point-to-Point Protocol (PPP).” RFC 1661 (Standards Track), July 1994.

[4] L. Blunk and J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP).” RFC 2284 (Standards Track), Mar. 1998.

[5] B. Aboba, “Extensible Authentication Protocol (EAP).” RFC 3748 (Standards Track), June 2004.

[6] W. Simpson, “PPP Challenge Handshake Authentication Protocol (CHAP).” RFC 1994 (Standards Track), Aug. 1996.

[7] G. Zorn and S. Cobb, “Microsoft PPP CHAP Extensions.” RFC 2433 (Standards Track), Oct. 1998.

[8] B. Aboba and D. Simon, “PPP EAP TLS Authentication Protocol.” RFC 2716 (Experimental), Oct. 1999.

[9] B. Aboba and M. Beadles, “The Network Access Identifier (NAI).” RFC 2486 (Standards Track), Jan. 1999.

[10] C. Rigney, S. Willens, A. Rubens, and W. Simpson, “Remote Authentication Dial In User Service (RADIUS).” RFC 2865 (Standards Track), June 2000.

[11] B. Anton, B. Bullock, and J. Short, “Best Current Practices for Wireless Internet Service Provider (WISP) Roaming,” Best Practices Document, Wireless Ethernet Compatibility Alliance (WECA), Wireless ISP Roaming (WISPr) Initiative, Mar. 2002.

[12] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, “Diameter Base Protocol.” RFC 3588 (Proposed Standard), Sept. 2003.

[13] Pass-One, “Pass-One Global Roaming Specification — General Description of WISP-provided Roaming Services,” Technical Specifications, Pass-One Consortium, May 2002, Draft 1.0.